

09/658, 565

日本特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出願年月日  
Date of Application:

2000年 1月25日



出願番号  
Application Number:

特願2000-016285

出願人  
Applicant(s):

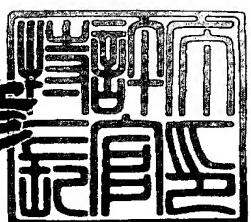
株式会社東芝

RECEIVED  
DEC 06 2000  
Technology Center 2  
JPO

2000年 6月 9日

特許庁長官  
Commissioner,  
Patent Office

近藤 隆彦



出証番号 出証特2000-3044301

【書類名】 特許願  
【整理番号】 A000000159  
【提出日】 平成12年 1月25日  
【あて先】 特許庁長官 殿  
【国際特許分類】 G09C 5/00  
【発明の名称】 埋め込み符号生成装置及び埋め込み符号検出装置とこれらを用いた電子透かし埋め込み装置及び電子透かし検出装置  
【請求項の数】 20  
【発明者】  
【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内  
【氏名】 村谷 博文  
【特許出願人】  
【識別番号】 000003078  
【氏名又は名称】 株式会社 東芝  
【代理人】  
【識別番号】 100058479  
【弁理士】  
【氏名又は名称】 鈴江 武彦  
【電話番号】 03-3502-3181  
【選任した代理人】  
【識別番号】 100084618  
【弁理士】  
【氏名又は名称】 村松 貞男  
【選任した代理人】  
【識別番号】 100068814  
【弁理士】  
【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【先の出願に基づく優先権主張】

【出願番号】 平成11年特許願第280652号

【出願日】 平成11年 9月30日

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705037

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 埋め込み符号生成装置及び埋め込み符号検出装置とこれらを用いた電子透かし埋め込み装置及び電子透かし検出装置

【特許請求の範囲】

【請求項1】

入力された利用者識別番号に対して、互いに素な複数の整数を法とする複数の剩余を求める剩余計算手段と、

前記剩余計算手段により求められた各剩余を表す符号であって、所定のビット数を一単位とする連續した1の列及び0の列で構成される複数の部分符号を生成する部分符号生成手段と、

前記部分符号生成手段により生成された各部分符号を連接して埋め込み符号を生成する連接手段とを具備することを特徴とする埋め込み符号生成装置。

【請求項2】

所定のビット数を一単位とする連續した1の列及び0の列で構成される複数の部分符号を連接した埋め込み符号を各部分符号に分割する符号分割手段と、

分割された各部分符号をそれぞれ復号して予め定められた互いに素な複数の整数を法とする2つの剩余からなる複数の剩余対を得る部分符号復号手段と、

前記複数の剩余対から結託者の利用者識別番号を計算する結託者番号計算手段とを具備することを特徴とする埋め込み符号検出装置。

【請求項3】

前記複数の剩余対から結託の有無を判定する結託判定手段をさらに有し、前記結託者番号計算手段は該結託判定手段により結託があると判定されたとき前記結託者の利用者識別番号を計算することを特徴とする請求項4記載の埋め込み符号検出装置。

【請求項4】

前記結託者番号計算手段は、入力された $k'$ 個の剩余対の各々から一方の剩余を選択して $k'$ 個の剩余の組( $r_1, r_2, \dots, r_{k'}$ )を生成する剩余選択部と

前記剩余選択部により生成された $k'$ 個の剩余の組から $k$ 個の剩余( $r_1, r$

2, ...,  $r_k$ )を選択する一貫性選択部と、

前記一貫性選択部により選択された  $k$  個の剩余から中国剩余定理に従って結託者の利用者識別番号  $u$  の候補を計算する中国剩余定理部とからなり、

前記一貫性検査部は、前記中国剩余定理部により計算された結託者の利用者識別番号  $u$  の候補と残りの  $(k' - k)$  個の剩余のうちの所定個数 ( $y$ ) の剩余との間に  $r_i = u \bmod p_i$  ( $i = 1, \dots, y$ ) が成立するか否かを判定し、この関係が成立する場合、 $u$  を結託の利用者識別番号として出力し、この関係が成立しない場合には前記剩余選択部に対して新たな  $k'$  個の剩余の組を要求し、結託者の利用者識別番号が特定できるまで新たな候補について同様の処理を繰り返すことを特徴とする請求項 1 または 2 記載の埋め込み符号検出装置。

#### 【請求項 5】

入力された利用者識別番号に対して複数の整数要素の組を計算する計算手段と、

所定個数の利用者識別番号に対して前記計算手段により計算される全ての整数要素の組を表現可能な  $k'$  個の部分符号のうちの  $k$  個の組み合わせが前記利用者識別番号を一意に表現できる部分符号を前記各整数要素に対応してそれぞれ生成する部分符号生成手段と、

前記部分符号生成手段により生成された各部分符号を連接して埋め込み符号を生成する連接手段とを具備し、

前記  $k'$  は、3 以上の正整数を  $c$ 、1 以上の正整数を、前記埋め込み符号の検出時に前記各部分符号から検出できる前記整数要素の個数を  $q$  として、 $c(k + 1)/q$  以上となるように決定されていることを特徴とする埋込み符号生成装置

#### 【請求項 6】

前記所定個数の利用者識別番号に対して前記計算手段により計算される各整数要素のとりうる値の個数を  $p_i$  ( $i = 1, 2, \dots, k'$ ) とし、前記埋め込み符号の検出時に想定される検出誤り率を  $\varepsilon$  としたとき、前記  $k'$  は、

## 【数1】

$$\left[ 1 - \prod_{i=1}^l \left\{ 1 - \left( 1 - \frac{1}{p_i} \right)^c \right\} \right]^{c(k+l)/2} C_{k+l} \times 2^{k+l} \geq 1 - \frac{\varepsilon}{2} \quad (1)$$

の条件を満たすように設定されていることを特徴とする請求項5記載の埋め込み符号生成装置。

## 【請求項7】

前記計算手段は、前記入力された利用者識別番号に対応して互いに素な複数の整数を法とする剩余の組を前記整数要素の組として計算することを特徴とする請求項5または6記載の埋め込み符号生成装置。

## 【請求項8】

前記計算手段は、前記入力された利用者識別番号に対応して平行移動によって定義される同値類に属する要素の番号の組を前記整数要素の組として計算することを特徴とする請求項5記載の埋め込み符号生成装置。

## 【請求項9】

前記計算手段は、前記入力された利用者識別番号に対応して平行移動によって定義される同値類に属する要素の番号の組を前記整数要素の組として計算するものであり、

前記  $p_i$  ( $i = 1, 2, \dots, k'$ ) を同一の正整数  $p$  として、

## 【数2】

$$k' = \frac{c}{2}(k+l) \leq \frac{p^k - 1}{p - 1} \quad (2)$$

の条件をさらに満たすことを特徴とする請求項6記載の埋め込み符号生成装置。

## 【請求項10】

所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能な  $k'$  個の部分符号のうちの  $k$  個の組み合わせが利用者識別番号を一意に表現できる部分符号であって、入力された利用者識別番号に対応して計算された整数要

素の組に対応して生成された部分を連接した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、

抽出された各部分符号に分割する符号分割手段と、

分割された各部分符号をそれぞれ復号する部分符号復号手段と、

各部分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、

前記  $k'$  は、3以上の正整数を  $c$ 、1以上の正整数を、前記埋め込み符号の検出時に前記各部分符号から検出できる前記整数要素の個数を  $q$  として、 $c(k+1)/q$  以上となるように決定されていることを特徴とする埋込み符号検出装置。

#### 【請求項11】

前記所定個数の利用者識別番号に対して計算される各整数要素のとりうる値を  $p_i$  ( $i = 1, 2, \dots, k'$ ) とし、前記埋め込み符号の検出時に想定される検出誤り率を  $\varepsilon$  としたとき、前記  $k'$  は、

#### 【数3】

$$\left[ 1 - \prod_{i=1}^l \left\{ 1 - \left( 1 - \frac{1}{p_i} \right)^c \right\} \right]^{c(k+1)/2} \geq 1 - \frac{\varepsilon}{2} \quad (1)$$

の条件を満たすように設定されていることを特徴とする請求項10記載の埋め込み符号検出装置。

#### 【請求項12】

前記整数要素の組は、前記利用者識別番号に対応して計算された互いに素な複数の整数を法とする剰余の組であることを特徴とする請求項10または11記載の埋め込み符号検出装置。

#### 【請求項13】

前記整数要素の組は、前記利用者識別番号に対応して計算された平行移動によって定義される同値類に属する要素の番号の組であることを特徴とする請求項1

0記載の埋め込み符号検出装置。

【請求項14】

前記整数要素の組は、前記利用者識別番号に対応して計算された平行移動によって定義される同値類に属する要素の番号の組であり、

前記  $p_i$  ( $i = 1, 2, \dots, k'$ ) を同一の正整数  $p$  として、

【数4】

$$k' = \frac{c}{2}(k+l) \leq \frac{p^k - 1}{p-1} \quad (2)$$

の条件をさらに満たすことを特徴とする請求項11記載の埋め込み符号検出装置

【請求項15】

所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能な  $k'$  個の部分符号のうちの  $k$  個の組み合わせが利用者識別番号を一意に表現できる部分符号であって、入力された利用者識別番号に対応して計算された整数要素の組に対応して生成された部分を連接した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、

抽出された各部分符号に分割する符号分割手段と、

分割された各部分符号をそれぞれ復号する部分符号復号手段と、

各部分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、

前記部分符号復号手段は、前記各部分符号をブロックに分割するブロック分割部と、該ブロック毎にブロック内の“1”的ビット数を計数する計数部と、該計数部で得られた計数値が第1の閾値を越えているか否かを判定する第1の判定部と、前記計数値が第2の閾値に満たないか否かを判定する第2の判定部と、前記第1の判定部で第1の閾値を越えていると判定された最小のブロックを決定する最小位置決定部と、前記第2の判定部で第2の閾値に満たないと判定された最大のブロックを決定する最大位置決定部とを有し、前記最小位置決定部及び最大値決定部の決定結果を復号結果として出力することを特徴とする埋め込み符号検出

装置。

【請求項16】

請求項1、5乃至9のいずれか1項に記載の埋め込み符号生成装置によって生成された埋め込み符号を埋め込み対象コンテンツに透かし情報として埋め込む電子透かし埋め込み装置。

【請求項17】

埋め込み対象コンテンツに対して利用者識別番号の情報を含む透かし情報を埋め込む電子透かし埋め込み装置において、

シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、

出力された符号語を前記透かし情報として前記埋め込み対象コンテンツに埋め込む手段と

を具備することを特徴とする電子透かし埋め込み装置。

【請求項18】

入力されたコンテンツから利用者識別番号の情報を含む透かし情報を検出する電子透かし検出装置において、

シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、

出力された符号語と前記コンテンツとの相関値を求める手段と、

前記相関値に基づいて前記コンテンツ中の前記入力された利用者識別番号に対応する符号語の有無を判定する手段と

を具備することを特徴とする電子透かし検出装置。

【請求項19】

入力されたコンテンツから利用者識別番号の情報を含む透かし情報を検出する電子透かし検出装置において、

予め登録された複数の利用者識別番号にそれぞれ対応する、シンプレックス符号を構成する複数の符号語を出力する手段と、

出力された各符号語と前記コンテンツとの各相関値を求める手段と、

求められた各相関値をベクトルとみなして計算されたノルムに基づいて前記コ

ンテンツ中の透かし情報の有無を判定し、透かし情報があると判定した場合に前記相関値に基づいて結託者を特定する手段と  
を具備することを特徴とする電子透かし検出装置。

#### 【請求項 20】

請求項 1 または 5 乃至 9 のいずれか 1 項に記載の埋め込み符号生成装置によって生成された埋め込み符号が透かし情報として埋め込まれたコンテンツを格納した記憶媒体。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、デジタルデータ化された音声、音楽、動画、静止画等のコンテンツに対して透かし情報を埋め込む電子透かし埋め込み装置及び埋め込み済コンテンツから透かし情報を検出する電子透かし検出装置に関する。

##### 【0002】

##### 【従来の技術】

電子透かし(digital watermarking)は、デジタルデータ化された音声、音楽、動画、静止画等のコンテンツに対して、これらのコンテンツの著作権者や利用者の識別情報、著作権者の権利情報、そのデータの利用条件、その利用時に必要な秘密情報、コピー制御情報などの情報(これらを透かし情報と呼ぶ)を知覚が容易ではない状態となるように埋め込み、後に必要に応じて透かし情報をそのデータ内から検出することによって利用制御、コピー制御を含む著作権保護を行ったり、二次利用の促進を行うための技術である。

##### 【0003】

##### [電子透かしの要件]

不正利用の防止を目的とする場合、電子透かし技術はデジタル著作物に対して通常に施されると想定される各種の操作や意図的な攻撃によって、透かし情報が消失したり改竄されたりしないような性質(ロバスト性)を持つ必要がある。例えば、静止画や動画はそれぞれ J P E G (Joint Photographic Coding Experts Group) 符号化、M P E G (Moving Picture Experts Group) 符号化と呼ばれる非可

逆圧縮を施されることが多いため、電子透かし技術はこれらの非可逆圧縮に対するロバスト性を持つことが重要な要件となることが通常である。

## 【0004】

## [電子透かしの分類]

従来、画像に対する電子透かしの方式は、画素領域利用型と周波数領域利用型に大別することができる。画素領域利用型の電子透かし方式は、画素値を変更することで直接的に透かし情報の埋め込みを行うものである。一方、周波数領域利用型の電子透かし方式は、直交変換によって、一旦、画素領域から周波数領域へ移り、周波数領域において埋め込みを行った後、再び、逆直交変換によって周波数領域から画素領域に戻るものである。透かし情報は波として埋め込まれることになる。

## 【0005】

## [周波数領域利用型電子透かし方式]

周波数領域利用型の電子透かし方式としては、例えば文献[1] Koch, E. and Zhao, J., "Towards Robust and Hidden Image Copyright Labeling", Proceedings of 1995 IEEE Workshop on Nonlinear Signal and Image Processing, 452-455, June 20-22, 1995.(Koch-Zhaoの方式という)や、文献[2]Cox, I.J., Kilian, J., Leighton, T. and Shamoon, T., "Secure Spread Spectrum Watermarking for Multimedia", NEC Research Institute, Technical Report 95-10, 1995.(Coxらの方式という)がある。これらの方では、埋め込み対象となる周波数成分を非可逆圧縮による影響が小さな低周波数から中間周波数に設定することで非可逆圧縮に対するロバスト性を実現している。

## 【0006】

## [画素領域利用型電子透かし方式]

画素領域利用型の電子透かし方式としては、画素値の LSB を変更することで埋め込みを行う方式がある。その変更は、擬似乱数系列(PN系列)に従って(文献[3] Schyndel, R.G. van, Tirkel, A.Z., and Osborne, C.F., "A Digital Watermark", Proceedings of 1st IEEE International Conference on Image Processing, 1994.あるいは文献[4] Wolfgang, R.B. and Delp, E.J., "A Water-

rmark for Digital Images” , ICIP96, 219-222, 1996.)、あるいは予め用意したマスクパターンに従って(文献[5] Pitas, I., “A Method for Signature casting on Digital Images” , ICIP96, 215-218, 1996.)、ある固定の大きさの変分を加えるか減ずるかを決定することで行う。この方式は、非可逆圧縮に対するロバスト性はあまり良くない。

## 【0007】

## [スペクトラム拡散による電子透かし]

スペクトラム拡散(spread spectrum)の考えを適用することで非可逆圧縮へのロバスト性を高める方式がある。スペクトラム拡散とは、通信したい信号に必要な帯域に比べて十分大きな帯域中に、情報を広く分散させて伝送する通信方式をいう(文献[6] 山内雪路, “スペクトラム拡散通信”, 東京電機大学出版局, 1994.)。伝送路上のノイズに対する耐性が優れている。元のコンテンツを搬送波、透かし情報を希望波、非可逆圧縮による影響を干渉波(ノイズ)とみなすことで、スペクトラム拡散の考えを電子透かし技術へ適用する。

## 【0008】

スペクトラム拡散による電子透かし方式として、画素領域における拡散(文献[7] Smith, J.R. and Comiskey, B.O., “Modulation and Information Hiding in Images” , Information Hiding, 207-226, 1996.)、文献[8]大西淳児, 岡一博, 松井甲子雄, “PN系列による画像への透かし署名” , SCIS97, 26B, 1997.)と、周波数領域における拡散(先の文献[2]参照)が提案されている。文献[2]の方式と文献[8]の方式は、それぞれ摂動法、直接拡散法(direct sequence spread spectrum)と呼ばれることがある(文献[9] 松井甲子雄, “電子透かしの基礎—マルチメディアのニュープロテクト技術—”, 森北出版株式会社, 1998.)。

## 【0009】

## [周波数領域における拡散(摂動法)]

先の文献[1]の方式では、透かし情報の埋め込みは画素値に対して直交変換を行い、周波数領域において透かし情報を拡散して埋め込む。拡散は、周波数領域において複数の周波数成分の値とある乱数列に従って変化させることによって行う。拡散後、逆直交変換を行う。透かし情報の検出は、画素値に対して直交変換

を行い、埋め込みが行われた周波数成分の値を埋め込みに用いられた乱数列の間の相関値によって判定を行う。埋め込まれた透かし情報は、画素領域では、画像(ブロック)全体に分散されているため、各種の操作に対してロバストである。また、透かし情報を埋め込んだ周波数成分が低中間周波数領域にあるならば、低周波数通過フィルタによっても透かし情報が失われにくい。

## 【0010】

## [画素領域における拡散(直接拡散法)]

一方、文献[8]の方式では、透かし情報の埋め込みは、P N (pseudo-random noise)系列を画素値に乗積することにより直接拡散する。得られた画像に対して直交変換を行い、周波数領域において透かし情報を埋め込み、再び逆直交変換を行う。その後、同じP N系列を画素値に乗積して、逆拡散を行う。透かし情報の検出は、P N系列によって画素値を直接拡散する。得られた画像に対して直交変換を行い、透かし情報の埋め込みを行った周波数成分の値から判定する。直接拡散法では、画素値をP N系列で変調するため、透かし情報は高周波成分に偏り、振動法と比較して、J P E G圧縮等やS t i r M a r k攻撃やD-A-D変換に対して、透かし情報が失われやすい。

## 【0011】

## [スペクトラム拡散の処理コストの軽減]

本発明者らは、J P E G圧縮等の下で透かし情報が失われにくくするために、透かし情報を埋め込むブロックサイズを大きくする方式を提案した(文献[10]村谷博文,加藤拓,遠藤直樹,“直接拡散による電子透かしの耐性評価”,SCIS99, II, 503-508, 1999.)。

## 【0012】

従来より、大きなブロックサイズの画像に対する埋め込みは行われていたが、この方式では大きなブロックに対する直交変換の処理コストを軽減することで埋込みおよび検出処理の低コストと高速性を実現した。この方式は、画像の周波数成分に依存しないか、あるいは、少数の周波数成分値にしか依存しない埋込み位置や埋込み強度を採用するため、振動法よりも直接拡散法に適していた。しかし、この方式は大きなブロックサイズを選択したため、大きなサイズの透かし情報

を埋め込むことが難しかった。

#### 【0013】

この問題に対しては、ブロック毎の画像の局所性に応じた埋め込みを行う「画像適応(image adaptation)」によって、小さな埋込み強度で埋め込みを行うことを可能にし、透かし情報のサイズを増加させる方法がある。この方法は例えば、文献[11] Boland, F.M., O Ruanaidh, J.J.K., and Dautzenberg, C., "Watermarking Digital Images for Copyright Protection", Proceedings of the fifth International Conference on Image Processing and its Application, 1995. (Boland等という)や、先の文献[8]に記載された方式で採用されている。

#### 【0014】

ところが、これら文献[11]や先の文献[8]の方式では、埋め込み強度は多数の周波数成分の値から決定されるため、本質的に直交変換を避けることができなくなってしまう。従って、直交変換を行うことなく、画素値から直接に埋め込み強度を決定する方式をとることが望ましい。

#### 【0015】

##### [フィンガープリンティング]

大きなサイズの透かし情報を JPEG圧縮等に対してロバストに埋め込むことができる電子透かし方式において、そのコンテンツ提供先の利用者を特定する情報を埋め込む応用形態が考えられる。このような応用形態は「フィンガープリンティング」と呼ばれる。海賊版の再配布を抑止する効果が期待できる。

#### 【0016】

##### [結託攻撃問題]

ところが、同じコンテンツに異なる透かし情報が埋め込まれた複数の埋め込み済みコンテンツが存在する場合、それら複数の埋め込み済コンテンツを利用して透かし情報を改竄、消失させるという行為が考えられる。このような行為は、「結託攻撃(collusion attack)」と呼ばれている。結託攻撃では、複数の埋め込み済みコンテンツの画素値を平均化することで新たなコンテンツを偽造したり、値が異なる画素値や周波数成分値の部分に対して、ランダムに、あるいは、多数決／少數決に従って値を変更する、などのやり方で改変を加える。

## 【0017】

## [結託攻撃に対する従来の対策]

従来、結託攻撃に対処する方法として、スペクトラム拡散による方法(先の文献[2]、及び文献[12]山本哲也、渡辺創、嵩忠雄、 “すべての結託ユーザを特定可能な電子透かし法” , SCIS'98, 10.2.B, 1998.)と、符号理論的な方法(文献[13] Boneh, Dan and Shaw, James, “Collusion-Secure Fingerprinting for Digital Data” , CRYPTO'95, 452-465, 1995.、文献[14]鈴置昌宏、渡辺創、嵩忠雄、 “結託攻撃に強い電子透かし法” , SCIS'97, 31B, 1997.及び文献[15]吉田淳、岩村恵市、今井秀樹、 “画質劣化が少なく結託攻撃に強い電子透かし法” , SCIS'98, 10.2.A, 1998.)が提案されている。

## 【0018】

文献[2]の方法によれば、利用者毎に  $N(0, 1)$  に従う相異なる実乱数列が与えられる。2つの異なる実乱数列の間に相関がないとする。結託攻撃は、画素値を平均化する操作とする。結託によって、検出時の相関値は減衰してしまう。

## 【0019】

文献[2]では、相関値の代わりに、定義された類似度によって結託の検出を行う。この類似度は、相関値を検出された透かし情報のノルムで除したものとして定義される。結託により電子透かしのノルムも減衰しているので、相関値が減衰しても類似度はさほど減衰しない。これにより結託者全員を特定することができる。ただし、この方法は検出において埋め込み対象であった原画像を必要とし、また結託者特定に時間がかかるのが難点である。

## 【0020】

文献[12]では、むしろ平均化による結託攻撃の際の相関値の減衰という性質を利用した結託者の特定方法を提案している。結託者間で共通の電子透かしは減衰せず、それ以外の電子透かしは減衰するので、埋め込み時のレベルを保っている電子透かしの組から結託者の組を特定する。全利用者数を  $n$ 、想定する最大の結託者数を  $c$  とすると、 $(c+1)(c-1) \log_{c+1} n$  オーダの長さの符号で結託者を特定することができる。ただし、この方法はスペクトラム拡散法に特有の性質を利用するため、すべての電子透かし方式に適用が可能なわけではない。

## 【0021】

先の文献[13]には、透かし情報を表現する符号において、すべての結託者の間で共通な値を持つビットは検出不能であるという性質を利用して、検出不能なビットがそのまま残るならば、それ以外のビットを如何に変更しようとも、結託者以外の利用者の符号を生成することができない符号(*c-frameproof*符号と呼ばれる)を構成して透かし情報とする方式が提案されている。

## 【0022】

この方式では、誰のものでもない符号が生成される可能性は残るもの、これにより、ある利用者が自らのコンテンツをそのまま再配布した場合(*native redistribution*)、その利用者は他者の結託によるものであると主張しての否認はできなくなる。

## 【0023】

結託者の総数に制限が無い*n-frameproof*符号は、符号サイズが  $n$  となる。結託者総数が最大  $c$  である *c-frameproof* 符号は、符号サイズが  $16c^2 \log n$  ( $c$  は結託者数、 $n$  は全利用者数) である。

## 【0024】

文献[13]ではさらに、2組の結託者のグループがあって、共通部分が空集合の場合、それぞれのグループ内の結託によって生成できる符号(*feasible set*)の集合間の共通部分も空集合であるような符号(*totally c-secure* 符号)は存在しないということを示している。つまり、結託攻撃によって誰のものでもない符号を生成することができない符号は、厳密には存在しないことを示した。

## 【0025】

そこで、文献[13]では結託者数が  $c$  人以内の場合に結託者を誤って指摘する確率が  $\varepsilon$  以下である符号(*c-secure code with  $\varepsilon$ -error*)を構成した。まず、誤り  $\varepsilon$  を持つ*n-secure* 符号  $\Gamma(n, 2n^2 \log(2n/\varepsilon))$  を構成した。その符号サイズは、 $2n^2(n-1)\log(2n/\varepsilon)$  である。

## 【0026】

さらに、それを*Traitor Tracing*スキーム(文献[16]Chor, B., Fiat, A. and Naor, M., “Tracing traitors”, Proceedings of CRYPTO’94, 257-270, 1994

.)と組合せて誤りが  $\varepsilon$  以下のc-secure符号の可能性を示した。この符号の符号サイズは、 $O(c^4 \log(n/\varepsilon) \log(1/\varepsilon))$  である。

## 【0027】

## [Chernoffの限界(Chernoff bound)]

文献[16]では、Traitor Tracingスキームにおいて、Chernoffの限界の式を利用して結託者を特定するために必要な利用者固有鍵の数を決定している。先の文献[13]では、その方法を流用して誤り  $\varepsilon$  のn-secure符号やc-secure符号を構成した。平均値  $p$  の独立な  $n$  個の確率変数  $X_i \in \{0, 1\}$  があるとき、これらの和が平均値からずれる確率の限界を与えるのがChernoffの限界である。上端と下端の限界は、それぞれ次式で与えられる。

## 【0028】

## 【数5】

$$\Pr\left[\sum_{i=1}^n X_i - np > n\delta\right] < \{\exp(\delta/p)/(1+\delta/p)^{1+\delta/p}\}^{np}$$

$$\Pr\left[\sum_{i=1}^n X_i - np < -n\delta\right] < \{\exp(-\delta/p)/(1-\delta/p)^{1-\delta/p}\}^{np}$$

## 【0029】

さらに、緩い限界として次式が成り立つ。

## 【0030】

## 【数6】

$$\Pr\left[\left|\sum_{i=1}^n X_i - np\right| > n\delta\right] < 2 \cdot \exp\{-\delta^2 n / (2p(1-p))\}$$

## 【0031】

ここで、 $0 \leq \delta < p(1-p)$  とする。また、次式が成り立つ。

## 【0032】

## 【数7】

$$\Pr\left[\sum_{i=1}^n X_i - np < -n\delta\right] < \exp\{-\delta^2 n / (2p^2)\}$$

## 【0033】

[結託者中の2人のみを指摘する方法]

文献[13]で提案されている誤り $\varepsilon$ のn-secure符号やc-secure符号は、できるだけ多数の結託者を指摘するように設計されていた。利用者を順序集合とみなし、文献[4]で示されている $\Gamma_0(n, d)$ 符号を、結託者の集合の中から最大と最小の2人を特定する符号として利用することもできる。この場合には、より小さな符号サイズでの構成が可能である。

## 【0034】

ここで、 $\Gamma_0(n, d)$ 符号とはdビットを一単位とする連続した1の列及び0の列で構成される符号であり、このような1の列や0の列を符号数nに応じた単位数だけ並べて構成される。従って、この符号では1と0はそれぞれdビットを単位として連続するように配置され、dビット未満の数の1や0が孤立して存在することはない。

## 【0035】

例えば、 $d = 3$ ,  $n = 5$ とすれば、 $\Gamma_0(n, d)$ 符号である $\Gamma_0(5, 3)$ 符号は以下のようになる。

1	1	1	1	1	1	1	1
0	0	0	1	1	1	1	1
0	0	0	0	0	0	1	1
0	0	0	0	0	0	1	1
0	0	0	0	0	0	0	0

文献[14]では、2つの符号を昇順と降順に重ね合わせた符号を利用し、結託者中の2人を特定するn-secure符号を提案している。この符号の符号サイズは、 $2n \log_4(2/\varepsilon) = n \log_2(2/\varepsilon)$ となる。文献[15]では、 $\Gamma_0(n, d)$ 符号において $0 < \text{weight}(x |_{Bs})$ となる最小のS( $S_{\min}$ )と、 $\text{weight}(x |_{Bs}) < d$ と

なる最大の  $S(S_{\max})$  を求め、 $S_{\min}$  と  $S_{\max} + 1$  を結託者であると指摘するアルゴリズムによって結託者の2人を特定する方法を示した。この符号の場合、誤り  $\epsilon$  の  $n$ -secure 符号は、符号サイズが  $(n - 1) \log_2(2/\epsilon)$  となる。

## 【0036】

[誤り  $\epsilon$  の 2-secure 符号]

結託者総数が小さな場合には、符号サイズを小さくすることが可能である。先の文献 [15] には、結託者総数 2 人の場合に結託者の両方を指摘する符号であって、その符号サイズが  $3n^{1/2} - 1 \log_2(6/\epsilon)$  の符号を示している。

## 【0037】

## [結託攻撃耐性の限界]

文献 [17] Ergun, Funde, Joe Kilian and Ravi Kumar, "A Note on the Limits of Collusion-Resistant Watermarking", EUROCRYPT'99, 140-149, 1999. は、電子透かし方式の詳細に依存せずに、結託攻撃に対する耐性には限界があることを理論的に示した。その主張は、正しい結託者を指摘する確率を高くしようとすると、誤った利用者を結託者として指摘してしまう確率(偽陽性率)が高くなってしまうというものであった。

## 【0038】

文献 [17] で想定している結託攻撃は、図 26 に示すように異なるすかし情報が埋め込まれた複数のコンテンツ(コンテンツ 1, コンテンツ 2, コンテンツ 3)を平均化し、その後、ランダムな擾乱を加えるというものである。Ergun 等の観点から、例えば先の文献 [13] での議論を捉えなおしてみる。文献 [13] における議論では、確率論的な  $c$ -secure 符号の構成要素として  $\Gamma_0(n, d)$  符号を用いている。この  $\Gamma_0(n, d)$  符号は、図 27 ( $d = 3$  の例) のように  $(1, 1, 1)$  と  $(-1, -1, -1)$  に符号をとる符号化を  $n$  重に直積して得られる。

## 【0039】

この  $\Gamma_0(n, d)$  符号に対して、文献 [17] で提案された結託攻撃を適用すると、平均化によって得られるコンテンツは、 $(1, 1, 1)$  と  $(-1, -1, -1)$  を結ぶ直線上にある重心に移る。結託攻撃は、さらに、その重心からずれた位置にコンテンツを移す。この場合、結託攻撃後のコンテンツが  $(1, 1, 1)$  か  $(-1, -1, -1)$  の近傍にあ

る場合には、これは結託攻撃によって変更されていないと判断し、原点付近にある場合には結託攻撃によって変更されたとみなすことになる。

## 【0040】

この $\Gamma_0(n, d)$ 符号において、結託者のうち(1,1,1)の符号を持つ者の数と(-1,-1,-1)の符号を持つ者の数の間に大きな偏りがある場合、平均化の結果、重心は(1,1,1)あるいは(-1,-1,-1)のかなり近くに位置することとなる。その後、ランダムな擾乱を受けるので、一般に、結託者を特定するアルゴリズムは、コンテンツが(1,1,1)または(-1,-1,-1)から擾乱によって移ったものか、重心から擾乱によって移ったものかを誤って判断する可能性が高い。つまり、Ergun等自身、かれらの結論がほとんどの電子透かしアルゴリズムに適用されると明言しているが、Boneh等の符号化もErgun等の限界を逃れることはできないといえる。

## 【0041】

一方、 $\Gamma_0(n, d)$ 符号において、2つの符号間の最大距離は $n d$ 、最小距離は $d$ と幅が大きい(図28参照)。 $\Gamma_0(n, d)$ 符号は結託攻撃への耐性に重点がおかれていることから、受信空間中に非常にスペースに符号語が配置されているためである。

## 【0042】

電子透かしアルゴリズムは、コンテンツの品質への影響がないように、符号間の最大距離 $n d$ の符号を埋め込む必要がある。電子透かしアルゴリズムが、 $\Gamma_0(n, d)$ 符号をコンテンツ空間へ埋め込み、その埋め込みが、符号間の距離とコンテンツ間の距離とが比例するような性質を持つ場合、オリジナルのコンテンツとの透かし情報を埋め込んだ後のコンテンツとの間の最大距離も $n d / 2$ 以上となるので、 $n d$ が大きな場合には、コンテンツ品質への影響が大きくなる(図29の埋め込み1)。

## 【0043】

仮に、これを避けるため、電子透かしアルゴリズムが符号をコンテンツ空間中のオリジナルコンテンツからの距離関係が保たれないような埋め込みによって、すべての符号語がオリジナルコンテンツとほぼ等しい距離にあるようにしたすると、 $\Gamma_0(n, d)$ 符号がもともと持っていた結託攻撃への耐性の根拠が失われ

てしまうことになる(図29の埋込み2)。

#### 【0044】

つまり、Ergun等の限界を意識した上で、結託攻撃に対する耐性の高さとコンテンツの品質への影響の小ささを適切に両立させた符号化による電子透かし方式を実現することが望ましいと考えられる。

#### 【0045】

(スペクトラム拡散による電子透かしの結託攻撃耐性)

一方、スペクトラム拡散による電子透かし方式では、埋め込みの影響がコンテンツ品質に大きな影響を与えないように埋め込み強度が設定される。その上で、埋め込みに用いる擬似乱数列が符号語に対応する。

#### 【0046】

標本値空間と周波数空間の間の直交変換は線形写像なので、攻撃対象の電子透かし方式が空間領域利用型であれ周波数領域利用型であれ、Ergun等の結託攻撃は擬似乱数列を平均化して、さらに擾乱を与えるという操作となる。

#### 【0047】

スペクトラム拡散による電子透かし方式では、符号語である擬似乱数列は相互相関(cross-correlation)がほとんどゼロとなるように選択されることが普通である。従って、 $k$ 個のコンテンツの平均によって得られるコンテンツは、ある結託者に対応する擬似乱数列との相関が $1/k$ に減衰すると考えられる。擬似乱数列間の相互相関が十分小さく、かつ、この $k$ があまり大きくなれば、電子透かしの検出において相関値があるあらかじめ定められた閾値を越えるため、結託者を特定することが可能である。

#### 【0048】

前述した文献[2]の方式は、検出においてオリジナルコンテンツを利用することを前提としており、相関値の代わりに類似度(similarity)と呼ばれる量を用いて検出が行われる。類似度は、検出対象コンテンツからオリジナルコンテンツを引いた差分と埋め込みに用いた擬似乱数列の間の相互相関値を差分の自己相関値の平方根で正規化したものである。

#### 【0049】

類似度による検出では、結託攻撃における平均化によって、分子の相関値が $1/k$ に減衰するが、分母の差分のノルムも $1/k$ に減衰するため、類似度は減衰しないことが期待される。ただし、平均化以外にノイズが加わる場合には、そのノイズの影響は正規化によってかえって大きくなる。

#### 【0050】

文献[18] Kilian, Joe, F.Thomas Leighton, Lesley R. Matheson, Talal G. Shamoon, Robert E. Tarjan, and Francis Zane, "Resistance of Digital Watermarks to Collusive Attacks", Technical Report TR-585-98, Department of Computer Science, Princeton University, 1998.では、統計的な議論によって文献[2]の電子透かし方式が何人までの結託者による結託攻撃に対する耐性を持っているかという理論的考察を行っている。疑似乱数系列はガウシアンノイズを仮定し、結託攻撃は結託者の持つコンテンツからオリジナルコンテンツを統計的に推定することで行うと仮定する。その結果、現実的なパラメータ設定で、数名から十数名の結託者に対する耐性を実現することが可能であるという結論が得られている。

#### 【0051】

また、電子透かしの応用形態によっては、オリジナルコンテンツを用いた検出が行えず、検出対象コンテンツのみから検出を行う必要がある場合がある。その場合には、類似度による検出は行えない。この場合には、許容される結託者の数はさらに小さくなると考えられる。

#### 【0052】

ところで、文献[2]や文献[18]での議論は、すべて、符号語である擬似乱数列の間の相互相関が十分小さいという前提に基づいている。しかし、一般に擬似乱数列の数が増えてくると、仮にそれをランダムに選択したとしても、偶然に大きな相互相関値を持つ対が生ずる可能性が高くなってくると思われる。

#### 【0053】

いったい、どの程度多くの擬似乱数系列が任意の対の間で相互相関値を小さくできるのか、また、そのような性質を持つ擬似乱数列をどのように選択すれば良いのか、そして、そのようにして選択された擬似乱数列を符号語として、どのよ

うな電子透かし方式を実現すれば、結託攻撃に強い方式となるのかが未解決の問題として残されている。

#### 【0054】

この問題も、先に[結託攻撃耐性]の項で述べた文献[17]での限界を意識した上で、結託攻撃に対する耐性の高さとコンテンツの品質への影響の小ささを適切に両立させた符号化による電子透かし方式をどう実現させるかという問題の一つと考えられる。

#### 【0055】

相互相関の小さな2値の擬似ランダムビット列を生成する方法として、M系列を利用する方法が知られている。M系列は、線形フィードバックシフトレジスタ(LFSR)の出力として得られる系列のうち、LFSRがGF(2)の原始多項式の係数に対応するタップを持つ場合に生成されるものである。M系列中の1と0をそれぞれ+1と-1に置き換えると、PN系列となる。M系列は、0の出現頻度が1の出現頻度がほぼ等しく(1の出現頻度が一回少ない)、その間の相互相関関数は0のとき値1、0以外のとき $-1/L$ となる。ここで、Lは系列の周期で、レジスタの段数をnとすると、 $L = 2^n - 1$ である。

#### 【0056】

M系列から得られたPN系列を巡回シフトして得られる系列を符号語として採用すれば、相互相関の小さな符号語が得られる。これらの符号語を電子透かしの埋め込みの際の擬似乱数系列として用いれば良い。この乱数系列は、空間領域利用型と周波数領域利用型の両方のスペクトラム拡散による電子透かしに利用できる。

#### 【0057】

周波数領域利用型のスペクトラム拡散の電子透かし方式では、普通、N(0, 1)に従うガウシアンノイズを符号語とする。相互相関が小さな符号語を複数構成するには、逐次乱数列を生成し、それが、それまでに生成したすべての乱数列との相関が小さいことを確認し、仮に、大きな相互相関値を持つ場合には、その乱数列は符号語として採用しないという方法をとる。

#### 【0058】

しかし、この方法では、新たに生成した乱数列がそれまでに生成した乱数列と小さな相互相関であるという保証がないため、せっかく生成した乱数列を捨てなければならないことがあるため処理が無駄である。特に、乱数列の数がある程度以上増えると、その確率は高くなる。

## 【0059】

## 【発明が解決しようとする課題】

以上に説明したように、従来の電子透かし技術では、結託攻撃によって透かし情報が失われたり偽造されたりすることで、不正な再配布が行われても、その不正行為者を特定できなくなる恐れがあった。

## 【0060】

また、結託攻撃へのロバスト性を実現する従来の提案において、非常に冗長な形で透かし情報を埋め込む必要があるため、あまり大きな利用者総数や結託者数を想定することができないという欠点があった。

## 【0061】

特に、J P E G圧縮等やその他の攻撃への耐性を持つ電子透かし埋め込み方式において、大きなサイズの透かし情報を埋め込むことはコンテンツの品質劣化を招く原因となる恐れがあった。

## 【0062】

さらに、結託者特定の際の埋め込み符号の検出誤りを正しく評価した上で透かし情報(埋め込み符号)を構成する必要があるが、従来の電子透かし技術ではこのような点に対する考察、特に3人以上の結託者が改竄に関与した場合の対策が不十分であり、また検出誤りに対して必要以上に透かし情報である埋め込み符号の符号サイズを大きくしてしまう可能性があった。

## 【0063】

本発明の目的は、結託攻撃への耐性を有し、利用者総数や結託者総数が大きな場合においても、コンテンツの品質劣化を極力抑えて透かし情報を埋め込む電子透かし埋め込み装置及び電子透かし検出装置を提供することにある。

## 【0064】

本発明の他の目的は、結託攻撃への耐性を有し、かつ3人以上の結託者が改竄

に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成する埋め込み符号生成装置及びその埋め込み符号を正しく復号する埋め込み符号検出装置を提供することにある。

## 【0065】

## 【課題を解決するための手段】

上記の課題を解決するため、本発明に係る第1の埋め込み符号生成装置は、入力された利用者識別番号に対して、互いに素な複数の整数を法とする複数の剰余を求める剰余計算手段と、この剰余計算手段により求められた各剰余を表す符号であって、所定のビット数を一単位とする連続した1の列及び0の列で構成される複数の部分符号を生成する部分符号生成手段と、この記部分符号生成手段により生成された各部分符号を連接して埋め込み符号を生成する連接手段とを具備することを特徴とする。

## 【0066】

この第1の埋め込み符号生成装置に対応する本発明に係る第1の埋め込み符号検出装置は、所定のビット数を一単位とする連続した1の列及び0の列で構成される複数の部分符号を連接した埋め込み符号を各部分符号に分割する符号分割手段と、分割された各部分符号をそれぞれ復号して予め定められた互いに素な複数の整数を法とする2つの剰余からなる複数の剰余対を得る部分符号復号手段と、前記複数の剰余対から結託者の利用者識別番号を計算する結託者番号計算手段とを具備することを特徴とする。

## 【0067】

また、複数の剰余対から結託の有無を判定する結託判定手段をさらに有し、この結託判定手段により結託があると判定されたとき、結託者番号計算手段が結託者の利用者識別番号を計算するようにしてもよい。

## 【0068】

結託者計算手段は、入力された  $k'$  個の剰余対の各々から一方の剰余を選択して  $k'$  個の剰余の組( $r_1, r_2, \dots, r_{k'}$ )を生成する剰余選択部と、この剰余選択部により生成された  $k'$  個の剰余の組から  $k$  個の剰余( $r_1, r_2, \dots, r_k$ )を選択する一貫性選択部と、この一貫性選択部により選択された  $k$  個の剰

余から中国剩餘定理に従って結託者の利用者識別番号  $u$  の候補を計算する中国剩  
余定理部とからなり、一貫性検査部は、中国剩餘定理部により計算された結託者  
の利用者識別番号  $u$  の候補と残りの  $(k' - k)$  個の剩余のうちの所定個数 ( $y$ ) の  
剩余との間に  $r_i = u \bmod p_i$  ( $i = 1, \dots, y$ ) が成立する場合があるか否かを判  
定し、この関係が成立する場合、 $u$  を結託の利用者識別番号として出力し、この  
関係が成立しない場合には剩余選択部に対して新たな  $k'$  個の剩余の組を要求し  
、結託者の利用者識別番号が特定できるまで新たな候補について同様の処理を繰  
り返す。

## 【0069】

本発明に係る第2の埋め込み符号生成装置は、入力された利用者識別番号に対  
応して複数の整数要素の組を計算する計算手段と、所定個数の利用者識別番号に  
対して前記計算手段により計算される全ての整数要素の組を表現可能な  $k'$  個の  
部分符号のうちの  $k$  個の組み合わせが前記利用者識別番号を一意に表現できる部  
分符号を前記各整数要素に対応してそれぞれ生成する部分符号生成手段と、この  
部分符号生成手段により生成された各部分符号を連接して埋め込み符号を生成す  
る連接手段とを具備し、前記  $k'$  は、3以上の正整数を  $c$ 、1以上の正整数を、  
前記埋め込み符号の検出時に前記各部分符号から検出できる前記整数要素の個数  
を  $q$  として、 $c(k+1)/q$  以上となるように決定されていることを特徴とし、  
より好ましくは前記所定個数の利用者識別番号に対して前記計算手段により計算  
される各整数要素のとり得る値を  $p_i$  ( $i = 1, 2, \dots, k'$ ) とし、前記埋め込  
み符号の検出時に想定される検出誤り率を  $\epsilon$  としたとき、前記  $k'$  は、

## 【0070】

## 【数8】

$$\left[ 1 - \prod_{i=1}^l \left\{ 1 - \left( 1 - \frac{1}{p_i} \right)^c \right\} \right]^{c(k+1)/2 C_{k,l} \times 2^{k+1}} \geq 1 - \frac{\epsilon}{2} \quad (1)$$

## 【0071】

の条件を満たすように設定されていることを特徴とする。

## 【0072】

ここで、前記計算手段は、例えば入力された利用者識別番号に対応して互いに素な複数の整数を法とする剩余の組を前記整数要素の組として計算するか、あるいは入力された利用者識別番号に対応して平行移動によって定義される同値類に属する要素の番号の組を前記整数要素の組として計算する。後者の場合、式(1)の条件に加え、前記  $p_i$  ( $i = 1, 2, \dots, k'$ ) を同一の正整数  $p$  として、

## 【0073】

## 【数9】

$$k' = \frac{c}{2}(k+l) \leq \frac{p^k - 1}{p - 1} \quad (2)$$

## 【0074】

の条件をさらに満たすことを特徴とする。

## 【0075】

第2の埋め込み符号生成装置に対応する本発明に係る第2の埋め込み符号検出装置は、所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能な  $k'$  個の部分符号のうちの  $k$  個の組み合わせが利用者識別番号を一意に表現できる部分符号であって、入力された利用者識別番号に対応して計算された整数要素の組に対応して生成された部分を連接した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、抽出された各部分符号に分割する符号分割手段と、分割された各部分符号をそれぞれ復号する部分符号復号手段と、各部分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、前記  $k'$  は、3以上の正整数を  $c$ 、1以上の正整数を、前記埋め込み符号の検出時に前記各部分符号から検出できる前記整数要素の個数を  $q$  として、 $c(k+1)/q$  以上となるように決定されていることを特徴とし、より好ましくは前記所定個数の利用者識別番号に対して計算される各整数要素のとりうる値を  $p_i$  ( $i = 1, 2, \dots, k'$ ) とし、前記埋め込み符号の検出時に想定される検出誤り率を  $\epsilon$  としたとき、前記  $k'$  は、式(1)の条件を満たすように設定されていることを特徴とする。

## 【0076】

ここで、前記整数要素の組は、例えば前記利用者識別番号に対応して計算された互いに素な複数の整数を法とする剰余の組、あるいは前記利用者識別番号に対応して計算された平行移動によって定義される同値類に属する要素の番号の組であり、後者の場合、式(1)の条件に加え、前記 $p_i$ ( $i = 1, 2, \dots, k'$ )を同一の正整数 $p$ として、式(2)の条件をさらに満たすことを特徴とする。

## 【0077】

本発明に係る第3の埋め込み符号検出装置は、所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能な $k'$ 個の部分符号のうちの $k$ 個の組み合わせが利用者識別番号を一意に表現できる部分符号であって、入力された利用者識別番号に対応して計算された整数要素の組に対応して生成された部分を連接した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、抽出された各部分符号に分割する符号分割手段と、分割された各部分符号をそれぞれ復号する部分符号復号手段と、各部分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、前記部分符号復号手段は、前記各部分符号をブロックに分割するブロック分割部と、該ブロック毎にブロック内の“1”的ビット数を計数する計数部と、該計数部で得られた計数値が第1の閾値を越えているか否かを判定する第1の判定部と、前記計数値が第2の閾値に満たないか否かを判定する第2の判定部と、前記第1の判定部で第1の閾値を越えていると判定された最小のブロックを決定する最小位置決定部と、前記第2の判定部で第2の閾値に満たないと判定された最大のブロックを決定する最大位置決定部とを有し、前記最小位置決定部及び最大値決定部の決定結果を復号結果として出力することを特徴とする。

## 【0078】

さらに、本発明によると上述した第1または第2の埋め込み符号生成装置によって生成された埋め込み符号を埋め込み対象コンテンツに透かし情報として埋め込む電子透かし埋め込み装置が提供される。

## 【0079】

本発明に係る他の電子透かし埋め込み装置は、埋め込み対象コンテンツに対し

て利用者識別番号の情報を含む透かし情報を埋め込む電子透かし埋め込み装置であって、シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、出力された符号語を透かし情報として埋め込み対象コンテンツに埋め込む手段とを具備することを特徴とする。

## 【0080】

本発明に係る他の電子透かし検出装置は、入力されたコンテンツから利用者識別番号の情報を含む透かし情報を検出する電子透かし検出装置であって、シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、出力された符号語とコンテンツとの相関値を求める手段と、この相関値に基づいてコンテンツ中の入力された利用者識別番号に対応する符号語の有無を判定する手段とを具備することを特徴とする。

## 【0081】

このような本発明に基づく埋め込み符号生成装置／埋め込み符号復号装置及び電子透かし埋め込み／検出装置においては、透かし情報である埋め込み符号の符号サイズを大きくすることなく、利用者総数や結託者数が大きくなても、結託攻撃に対するロバスト性を得ることができる。

## 【0082】

また、 $k' \geq c(k+1)/q$ 以上という条件、さらには式(1)や式(2)の条件を満たすようにすることによって、3人以上の結託者が改竄に関与した場合においても、埋め込み符号検出時の正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成する埋め込み符号生成装置及びその埋め込み符号を正しく復号する埋め込み符号復号装置が実現される。

## 【0083】

## 【発明の実施の形態】

図1は、本発明の電子透かし埋め込み装置1と電子透かし検出装置2が適用されるシステムの例であるフィンガープリンティングシステムの概念図を示す。

画像や音声などの埋め込み対象コンテンツと利用者識別番号が電子透かし埋め

込み装置1に入力され、ここで得られた埋め込み済みコンテンツがこれを格納する記憶媒体を含む流通経路3を経て流通する。

## 【0084】

前述した結託攻撃は、流通経路3において埋め込みコンテンツに対して行われる。このような結託攻撃に対抗するために、本発明に基づく電子透かし検出装置2では、結託の有無を示す結託判定信号、結託があった場合の結託者を特定する結託者番号(結託者の利用者識別番号)、及び結託がなかった場合の正規の利用者識別番号が生成される。

## 【0085】

以下、本発明による電子透かし埋め込み装置及び電子透かし検出装置の実施形態について説明する。

## (第1の実施形態)

本発明の第1の実施形態として、従来例よりも小さな符号サイズを持つε誤りのc-secure符号による電子透かし埋め込み装置及び電子透かし検出装置について説明する。

図2は、本発明の第1の実施形態に係る電子透かし埋め込み装置の概略構成を示している。この電子透かし埋め込み装置は、埋め込むべき透かし情報である利用者識別番号の埋め込み符号を生成する埋め込み符号生成部11と、生成された埋め込み符号を埋め込み対象コンテンツに埋め込み、埋め込み済みコンテンツを得る符号埋め込み部12とからなる。

## 【0086】

図3は、埋め込み符号生成部11の構成を示している。この埋め込み符号生成部11は、それぞれk'個の法記憶部21-1, 21-2, …, 21-k'、剩  
余計算部22-1, 22-2, …, 22-k'、部分符号生成部24-1, 24-2, …, 24-k' と、符号パラメータ記憶部23及び符号連接部25からなる。

## 【0087】

法記憶部21-1, 21-2, …, 21-k'には互いに素な整数、この例では相異なるk'個の素数 $p_i$ ( $i = 1, 2, \dots, k'$ )が法として記憶されており

、剩余計算部 22-1, 22-2, …, 22-k' は、入力される利用者識別番号  $u$  に対して、これらの素数  $p_i$  を法とする剩余  $u_i = u \bmod p_i$  ( $i = 1, 2, \dots, k'$ ) をそれぞれ求める。すなわち、入力された利用者識別番号に対応した複数の整数要素の組として、剩余計算部 22-1, 22-2, …, 22-k' により剩余  $u_i = u \bmod p_i$  ( $i = 1, 2, \dots, k'$ ) が計算される。

## 【0088】

部分符号生成部 24-1, 24-2, …, 24-k' は、 $k'$  個の素数  $p_i$  ( $i = 1, 2, \dots, k'$ ) に対して、符号パラメータ記憶部 23 に記憶された符号パラメータ  $d$  に従って剩余計算部 22-1, 22-2, …, 22-k' により求められた剩余  $u_i$  ( $i = 1, 2, \dots, k'$ ) を表す前述した  $\Gamma_0(n, d)$  符号からなる部分符号  $\Gamma(p_i, 1)$  をそれぞれ生成する。すなわち、部分符号生成部 24-1, 24-2, …, 24-k' では、所定個数 ( $n$ ) の利用者識別番号に対して剩余計算部 22-1, 22-2, …, 22-k' で計算される全ての剩余  $u_i$  ( $i = 1, 2, \dots, k'$ ) の組を表現可能な  $k'$  個の部分符号のうちの  $k$  個の組み合わせが利用者識別番号を一意に表現できる部分符号  $\Gamma(p_i, 1)$  を各剩余に対応して生成する。

## 【0089】

符号連接部 25 は、部分符号生成部 24-1, 24-2, …, 24-k' により生成された各部分符号  $\Gamma(p_i, 1)$  を連接することによって、透かし情報である埋め込み符号を生成する。

## 【0090】

図4に、部分符号生成部 24-1, 24-2, …, 24-k' の一つ (24-i) の構成を示す。符号パラメータを  $d$ 、剩余を  $u_i$ 、法を  $p_i$  とすると、減算部 31 では  $p_i - u_i - 1$  が求められる。“0”列生成部 32 では、符号パラメータ  $d$  と剩余  $u_i$  に基づき  $d \times u_i$  ビットの連續した“0”列が生成され、“1”列生成部 33 では、符号パラメータ  $d$  と減算部 31 からの出力  $p_i - u_i - 1$  に基づき  $d \times (p_i - u_i - 1)$  ビットの連續した“1”列が生成される。そして、これらの“0”列と“1”列が連接部 34 で連接され、 $d \times (p_i - 1)$  ビットのビット列が  $\Gamma_0(n, d)$  符号からなる部分符号  $\Gamma(p_i, 1)$  として生成される。

## 【0091】

図20は、こうして生成される部分符号の一例を示している。0から $n-1$ までのn個の利用者識別番号に対応して、 $B(0), \dots, B(n-2)$ のブロック“0”列からなる部分符号が割り当てられている。

## 【0092】

図5に、本実施形態に係る電子透かし検出装置の構成を示す。この電子透かし検出装置は、透かし情報抽出部41、符号分割部42、部分符号復号部43-1, 43-2, …, 43-k'、利用者識別番号計算部44、結託判定部45-1, 45-2, …, 45-k'、結託判定OR部46及び結託者番号計算部47から構成されている。

## 【0093】

透かし情報抽出部41では、入力された埋め込み済みコンテンツから透かし情報(埋め込み符号)が抽出され、この抽出された透かし情報である埋め込み符号が符号分割部42により各部分符号に分割された後、部分符号復号部43-1, 43-2, …, 43-k'により復号されることにより、利用者識別番号に対応する剩余対が生成される。

## 【0094】

こうして生成された各剩余対の一方の剩余から、利用者識別番号計算部44により利用者識別番号が計算で求められ、また各剩余対から結託判定部45-1, 45-2, …, 45-k'により結託の有無が判定される。結託判定部45-1, 45-2, …, 45-k'の判定結果について、結託判定OR部46で論理和がとられることにより、結託が存在したか否かが最終的に判定される。さらに、結託が存在すると判定されたときは各剩余対から結託者番号計算部47で結託者番号が計算され、結託者が特定される。

## 【0095】

図6に、結託者番号計算部47の詳細な構成を示す。この結託者番号計算部47は、 $k'$ 個の剩余対から各一つの剩余を選択する剩余選択部51と、選択された $k'$ 個の剩余のうち $k$ 個の剩余を選択する一貫性検査部52、及び一貫性検査部52で選択された $k$ 個の剩余に対して中国剩余定理を適用して結託者番号候補

を得る中国剩余定理部53からなる。

#### 【0096】

図7に、図6中の一貫性検査部52の内部構成を示す。中国剩余定理部53により得られた結託者番号候補は一貫性検査部52にフィードバックされ、 $k'$ 個の剩余のうち残りの( $k' - k$ )個の剩余との間の一貫性検査が行われて、最終的に結託者番号が求められる。図7の一貫性検査部52は、剩余の( $k + 1$ )組の生成部521と、剩余の1組と結託者番号候補の一貫性検査部522から構成される。その動作については、後に説明する。

#### 【0097】

本実施形態の電子透かし埋め込み装置及び電子透かし検出装置によると、利用者総数や結託者総数が大きい場合においても、コンテンツの品質劣化の少ない電子透かしが可能となる。以下、詳細に説明する。

利用者総数をnとし、結託者総数の最大値をcとする。一方、図3の法記憶部21-1, 21-2, …, 21-k'で用意されている $k'$ 個の素数 $p_1, p_2, \dots, p_{k'}$ から任意のk個の素数を選んだとき、それらのk個の素数の積はn以上とする。例えば、この積は $n \leq p_1 \times p_2 \times \dots \times p_k$ である。

#### 【0098】

埋め込み符号生成部12では、各素数 $p_i$ ( $i = 1, 2, \dots, k'$ )に対して、図3の部分符号生成部24-1, 24-2, …, 24-k'により部分符号 $\Gamma(p_i, 1)$ が生成される。これらの部分符号 $\Gamma(p_i, 1)$ を符号連接部25により連接することによって、新たな符号 $\Gamma(p_1, p_2, \dots, p_{k'} : 1)$ が生成される。

#### 【0099】

ここで、各利用者の利用者識別番号をuとすると、その利用者識別番号uに対応する連接符号 $\Gamma(p_1, p_2, \dots, p_{k'} : 1)$ の符号語は、各部分符号 $\Gamma(p_i, 1)$ がその利用者識別番号uに対する素数 $p_i$ を法とする、剩余計算部22-1, 22-2, …, 22-k'で計算された剩余 $u \bmod p_i$ を表す符号語となり、これが透かし情報(埋め込み符号)として埋め込み対象コンテンツに埋め込まれることになる。

#### 【0100】

このようにして得られた埋め込み済みコンテンツに対して結託攻撃が行われた場合、図5の電子透かし検出装置において、符号分割部42で分割された各部分符号 $\Gamma(p_i, 1)$ を部分符号復号部43-1, 43-2, …, 43-k'で復号することによって、c人中のある2人の利用者識別番号の $p_i$ に関する剩余(residue)の対が得られる。これを $p_i$ に関する剩余対(residue pair)と呼ぶことにする。

## 【0101】

また、 $p_i$ に関する剩余対中のある剩余がある利用者識別番号uを保有する結託者の剩余であるとき、その剩余は利用者識別番号uを保有する結託者に起因すると呼ぶことにする。このとき、この結託者を含めて結託者と同じ剩余の値を持つ利用者に関しては、その剩余はその利用者の利用者識別番号に起因する可能性があると呼ぶことにする。

## 【0102】

(補題1) c人以下の結託において、 $\Gamma(p_1, p_2, \dots, p_{k'} : 1)$ により $k'$ 個の相異なる素数に関する剩余対が与えられたとき、それらの剩余対中に、ある結託者の利用者識別番号に起因する剩余の数が $2k' / c$ 以上含まれるような結託者が少なくとも1人存在する。

## 【0103】

(補題2) 剩余対中のある剩余に、結託により誤りを生じる確率を $\varepsilon$ 以下とするには、 $1 \geq \log_2(1 / \varepsilon)$ でなければならない。

## 【0104】

(系1)  $k'$ 個の剩余対に含まれる剩余のどの一つの剩余にも、結託によって誤りが生じない確率を $\varepsilon$ 以下とするには、 $1 \geq \log_2(2k' / \varepsilon)$ でなければならない。

## 【0105】

(補題3) 符号 $\Gamma(p_1, p_2, \dots, p_{k'} : 1)$ は、結託により誤った符号を生じない確率を $\varepsilon$ 以下とするには、 $1 \geq \log_2(2k' / \varepsilon)$ 、つまり、符号サイズLは、次式でなければならない。

## 【0106】

【数10】

$$L \geq \left( \sum_{i=1}^{k'} p_i \right) \times \log_2 (2k' / \varepsilon) \quad (3)$$

【0107】

以下、 $p_m = \min(p_1, \dots, p_{k'})$ 、 $p_M = \max(p_1, \dots, p_{k'})$ とし、また

【数11】

$$\langle P \rangle = \sum_{i=1}^{k'} p_i / k' \quad (4)$$

【0108】

とする。符号サイズの下限は、 $L = k' \times \langle P \rangle \times \log^2(2k' / \varepsilon)$ と表わされる。

【0109】

(中国剩余定理(Chinese Remainder Theorem))

相異なる  $k$  個の素数  $p_1, p_2, \dots, p_k$  が与えられたとき、各  $i$  ( $i = 1, 2, \dots, k$ ) について  $u_i \in Z_{p_i}$  が与えられると、 $u_i \equiv u \pmod{p_i}$  である  $u \in Z_{p_1} \times Z_{p_2} \times \dots \times Z_{p_k}$  が一意に定まり、帰納的に計算できる。これが中国剩余定理である。

【0110】

中国剩余定理を適用すると、図6に示すように中国剩余定理部53に  $k'$  個の素数のうち  $k$  個の素数に対応する剰余が与えられれば、それから利用者識別番号を一意に定めることができる。しかし、それらの剰余すべてが同一結託者の利用者識別番号に起因するとは限らないため、求めた利用者識別番号が結託者を正しく特定するとは限らない。

【0111】

そこで、さらに余分に 1 個の剰余を用意し、 $(k + 1)$  個の剰余の間の一貫性を検査することで、得られた利用者識別番号の正当性を検証する。言い換えると、 $(k + 1)$  個の建立合同方程式の解の存在を確認する。例えば、 $k$  個の剰余から得

られた利用者識別番号に対して、残りの剩余  $r_{k+1}, \dots, r_{k+1}$  に対応する整数  $p_{k+1}, \dots, p_{k+1}$  で除した余り(remainder)を求め、それらがそれぞれ剩余  $r_{k+1}, \dots, r_{k+1}$  に一致し、一致したか否かで結託者を判定することとする。

## 【0112】

すなわち、図6の一貫性検査部52では図7に示すように、図6の剩余選択部51で  $k'$  個の剩余対から各一つ選択された  $k' = c(k+1)/2$  個の剩余を剩余の  $(k+1)$  組の生成部521に入力し、これら  $k'$  個の剩余の中から  $k$  個の剩余を選択して中国剩余定理部53に引き渡す。さらに、一貫性検査部522により剩余の1組と結託者番号候補との一貫性検査を行って、結託者番号(結託者の利用者識別番号)を出力する。

## 【0113】

結託者数が2人の場合については、この方法を比較的容易に実現できる(例えば、特願平10-108039、特願平10-122108)。ここでは、それを一般の結託者数に拡張する。

## 【0114】

$m$  個の素数に対応する剩余の組( $m$ -tuple of residues)の中の任意の  $k$  個の剩余に対して中国剩余定理を適用したとき、これら  $m$  個の剩余の組がすべて同一の利用者識別番号を与える場合、このような剩余の組を一貫している(consistent)と呼ぶことにする。

## 【0115】

さらに、このような一貫している剩余の組の全ての剩余が、求められた結託者の利用者識別番号に起因している場合、この剩余の組は真に一貫している(truly consistent)と呼び、そうでない場合、この剩余の組は偽って一貫している(falsely consistent)と呼ぶことにする。このような偽って一貫している組の簡単な例を以下に挙げる。

一貫している  $m$  個の剩余に対して、さらに第  $(m+1)$  番目の素数  $p$  に関する剩余を加えて  $(m+1)$  個の剩余としたとき、それらが一貫している確率は、新たに加えた素数  $p$  に関する剩余がランダムに値をとる場合には、 $1/p$  となる。

## 【0116】

従って、 $m$ 個の剩余対から各1個の剩余を選択して、 $m$ 個の剩余を構成する場合、偶然に、偽って一貫した $m$ 個の剩余が得られる確率は、 $m$ を大きくするにつれて小さくなり、その確率は $(2/p_m)^{m-k}$ より小さくなる。ただし、 $m > k$ とする。

## 【0117】

(系2) 偽って一貫した剩余の組が得られる確率を $\varepsilon$ 以下とするには、 $m \geq k + \log_{p_m/2}(1/\varepsilon)$ とすればよい。

ここで、系2から、偽って一貫した剩余の組が得られる確率を $\varepsilon$ 以下とするためには、 $m \geq k + \log_{p_m/2}(1/\varepsilon)$ 個の同一利用者に起因する剩余を含む剩余対を用意すれば良い。(補題1)から、それには $k' \geq (c/2) \times (k + \log_{p_m/2}(1/\varepsilon))$ の剩余対を用意すれば良い。

## 【0118】

結託者を正しく決定するには、剩余対が正しく得られた上で真の一貫した組を得る必要がある。そこで、それぞれの誤り率 $\varepsilon$ を $\varepsilon'$ と以下とすると、結託者を正しく決定できない確率は $(\varepsilon + \varepsilon')$ 以下となる。そこで、 $\varepsilon \rightarrow \varepsilon/2$ 、 $\varepsilon' \rightarrow \varepsilon/2$ と再定義して、次の定理を得る。

## 【0119】

(定理1) 符号 $\Gamma(p_1, p_2, \dots, p_{k'} : 1)$ が、誤り率 $\varepsilon$ 以下で結託者を正しく決定するには、 $k' \geq (c/2) \times (k + \log_{p_m/2}(2/\varepsilon))$ 、 $1 \geq \log_2(4k'/\varepsilon)$ を満たせば良い。

よって、(補題3)よりその符号サイズの下限は、

$$\begin{aligned} L = & \langle p \rangle \times (c/2) \times (k + \log_{p_m/2}(2/\varepsilon)) \\ & \times \log_2((2c/\varepsilon) \times (k + \log_{p_m/2}(2/\varepsilon))) \end{aligned}$$

で与えられる。

## 【0120】

ここで、すべての素数がほぼ同じ大きさとなるように選択する。 $p_i = p$ とすると、 $p = \langle p \rangle = n^{1/k}$ 。よって、符号サイズの下限は、

$$\begin{aligned} L = & (c/2) \times n^{1/k} \times (k + \log_n^{1/k}/2(2/\varepsilon)) \\ & \times \log_2((2c/\varepsilon) \times (k + \log_n^{1/k}/2(2/\varepsilon))) \end{aligned}$$

で近似される。

## 【0121】

さらに、ある正数  $a$  を選び、 $k = (\log_2 n) / a$  と設定することができるならば、符号サイズの下限は、

$$L \doteq (c e^a / 2a) \times (\log_2 n + a \times \log_e a / 2(2/\varepsilon)) \\ \times \log_2((2c/\varepsilon a) \times (\log_2 n + a \times \log_e a / 2(2/\varepsilon)))$$

で近似される。この場合、符号サイズの下限は  $c$  に関して  $\Theta(c \log_2 c)$ 、 $n$  に関して  $\Theta(\log_2 n \log_2 \log_2 n)$  となり、例えば先の文献[14]や文献[15]に開示された従来の方式と比較して、最も小さなオーダーとなる。

## (素数定理(prime number theorem))

自然数  $x$  を超えない素数の個数を  $\pi(x)$  とすると、 $\pi(x) \doteq x / \log x$  となる。先ほどの符号化では、 $k = (\log_2 n) / a$  とした。そこで、素数定理より  $\delta$  を小さな正数とするとき、 $x \sim x(1 + \delta)$  の間に素数が  $\log_2 x$  オーダーの個数以上存在することは、次のように確認できる。

## 【0122】

$$\pi(x + (1 + \delta)) - \pi(x) \doteq (x / (\log x - 1) / \log^2 x) \\ = \omega(\log x)$$

次に、上の定理1が前提としている、結託者を特定するアルゴリズムについて図8に示すフローチャートを用いて説明する。

結託者番号計算部47は、部分符号復号部43-1, 43-2, …, 43-k' が output した  $k'$  個の剩余対を入力する(ステップS1)。剩余対は、まず剩余選択部51に入力される。剩余選択部51は、各剩余対から一方の剩余を選択し、 $k$  個の剩余の組( $r_1, r_2, \dots, r_k'$ )を生成する(ステップS2)。

## 【0123】

生成された  $k'$  個の剩余の組は、一貫性検査部52に入力される。一貫性検査部52は、入力された  $k'$  個の剩余の組から  $k$  個の剩余( $r_1, r_2, \dots, r_k$ )を選択し(ステップS3)、中国剩余定理部53に渡す。

## 【0124】

中国剩余定理部53は、中国剩余定理に従い結託者番号  $u$  を計算する(ステッ

プS4)。この中国剩余定理の計算は、図9のフローチャートに示す処理の流れに従って行われる。計算された結託者番号uは、一貫性検査部52へ返される。

#### 【0125】

一貫性検査部52では、残りの( $k' - k$ )個の剩余のうちの所定個数(y)の剩余との間に、 $r_i = u \bmod p_i$  ( $i = 1, \dots, y$ )が成立する場合があるか否かを判定する(ステップS5)。この関係が成立する場合、一貫性検査部52はuを結託者番号として出力する(ステップS6)。この関係が成立しない場合には、一貫性検査部52は剩余選択部51に対して、新たな $k'$ 個の剩余の組を要求する(ステップS7)。もし、新たな候補が存在しない場合には、結託者番号の特定に失敗したことになる(ステップS8)。

#### 【0126】

最後に、図10に示すフローチャートを用いて本実施形態における電子透かし検出装置の流れについて説明する。

埋め込み済みコンテンツが入力され(ステップS11)、この埋め込み済みコンテンツから透かし情報抽出部41で透かし情報である埋め込み符号が検出されると(ステップS12)、符号分割部42及び部分復号部43-1, 43-2, ..., 43 $k'$ を介して得られた部分符号に基づいて、結託判定部45-1, 45-2, ..., 45- $k'$ により結託の有無が判定される(ステップS13)。

#### 【0127】

ここで、結託判定部45-1, 45-2, ..., 45- $k'$ のいずれでも結託がないと判定されると、利用者識別番号計算部44により利用者識別番号が計算され(ステップS14)、この利用者識別番号が出力される(ステップS15)。

#### 【0128】

一方、ステップS13で結託判定部45-1, 45-2, ..., 45- $k'$ の少なくとも一つで結託が有ると判定されると、結託判定部46を介して結託存在信号が出力され(ステップS16)、かつ結託者番号計算部47で結託者番号が計算され(ステップS17)、この結託者番号が出力される(ステップS18)。

#### 【0129】

この場合、ステップS13での結託の有無の判定と、ステップS14での利用

者識別番号の計算については、処理が簡単であり、高速に行うことができる。これに対して、ステップS17での結託者番号の計算には時間がかかるが、結託の有無の判定を先に行い、結託が有ったと判断された場合にのみ結託者番号の計算を行うことにより、無駄な計算を省略できる。

## 【0130】

また、本発明の電子透かし検出装置を利用者機器に適用する場合には、結託の有無のみを判定し、その結果によって利用を中断させるなどの利用制御を行えばよいので、結託者の計算(特定)まで行う必要は必ずしもない。

## 【0131】

このように本実施形態によると、埋め込むべき符号サイズを抑えつつ、利用者総数や結託者数が大きい場合についても、結託攻撃に対するロバスト性を持つことができる。

## 【0132】

## (第2の実施形態)

次に、上述した第1の実施形態を改良した本発明の第2の実施形態として、結託者特定の際の誤り率評価をより厳密にして必要な個数のみの素数を用意し、かつ符号サイズをより効果的に削減できる電子透かし埋め込み装置及び検出装置について説明する。

## 【0133】

第1の実施形態では、結託者の特定に際して埋め込み符号検出時の誤り評価を厳密に行っておらず、必ずしも用意すべき複数の素数(互いに素な整数)の個数の下限が正しく求められていない。また、用意すべき素数の個数が大きくなると、用意する最も小さな素数と比べて大きな素数まで用いる必要が生じるため、符号サイズ削減の効果が殺がれてしまう。第2の実施形態によると、このような課題を解決することができる。

## 【0134】

本実施形態に係る電子透かし埋め込み装置及び検出装置の構成は、第1の実施形態と基本的に同様であり、本実施形態では電子透かし埋め込み装置の部分符号生成部及び電子透かし検出装置の部分符号復号部として必要な個数(部分府古豪

の数)について述べる。

## 【0135】

利用者総数を  $n$  とし、結託者の最大数を  $c$  とする。先の文献 [13] によって導入された  $\epsilon$  誤りを持つ  $n$ -secure 符号 (cubic length  $n$ -secure code with  $\epsilon$ -error) は、以下のように定義される。

## 【0136】

(定義 1)  $((n - 1)d, n)$  符号  $\Gamma_0(n, d)$  は、その符号語  $w^{(0)}, \dots, w^{(n-1)}$  が次の条件を満たす符号と定義する。

## 【0137】

## 【数12】

$$w^{(i)}|_{B_j} = \begin{cases} \{0\}^d & \text{for } i > j \\ \{1\}^d & \text{otherwise} \end{cases} \quad (5)$$

## 【0138】

ここで、 $w^{(i)}|_{B_j}$  は符号語  $w^{(i)}$  をビット位置の集合  $B_j$  に制限したものである。集合  $B_i, i = 0, \dots, n - 2$  はブロック (blocks) と呼ばれ、 $d$  個のビット位置から構成される。異なるブロック間は共通部分を持たない ( $i \neq j$  に対して  $B_i \cap B_j = \emptyset$ )。

## 【0139】

すべての利用者に対して、シリアル番号のような形で順序をつけることができると仮定する。 $i$  番目の利用者に対して、符号語  $w^{(i)}$  を割り当てるとする。さらに、利用者は自分に割り当てられたシリアル番号を知らされていないとする。

## 【0140】

先の文献 [12] [14] によって導入された  $\epsilon$  誤りを持つ線形  $n$ -secure 符号 (linear length  $n$ -secure code with  $\epsilon$ -error) は、符号語は定義 1 で定義された符号と同一であるが、検出アルゴリズムが異なる。この符号は、結託者中で最大と最小のシリアル番号をもつ 2 人の結託者を特定することができる。符号サイズは  $\Theta(n)$  である。

## 【0141】

(定理2) 以下の検出アルゴリズム1を符号 $\Gamma_0(n, d)$ に適用するとする。 $d = \log_2(2/\varepsilon)$ ならば、この符号は $\varepsilon$ 誤りを持ったn-secure符号である。

## 【0142】

(検出アルゴリズム1)

(1) 検出された符号 $x \in \{0, 1\}^l$ を入力する。ここで、 $l = (n - 1)d$ 、 $d = \log(1/\varepsilon)$ とする。

(2)  $s = 1$ から $n - 1$ まで、以下を実行する：

(2-1)もし、 $x|_{Bs} \neq \{0\}^d$ ならば中断する。

(3)  $t = n$ から $s$ まで、以下を実行する：

(3-1)もし、 $x|_{Bi-1} \neq \{0\}^d$ ならば中断する。

(4)  $s$ と $t$ を出力する。

## 【0143】

$k, k'$ ,  $l$ は、 $k' = c(k + 1)/2$ を満足する正整数とする。 $p_1, \dots, p_k$ は、互いに素な整数とする。 $p$ は $p_1, \dots, p_k'$ のうち最小のものとする。また、 $p_1, \dots, p_k'$ のうち小さい方から選んだ $k$ 個の積を $n$ 以上とする。これらの整数 $p_1, \dots, p_k'$ を以下では因数と呼ぶことにする。

## 【0144】

これらの因数の平均値を $p_{ave}$ とする( $p_{ave} = p_1 + \dots + p_k'/k'$ )。 $i = 1, \dots, k'$ の各 $p_i$ に対応して、先の文献[13]のn-secure符号 $\Gamma_0(p_i, t)$ を構成要素の符号として用意する。

## 【0145】

(定義2)  $((p_{ave} - 1)k', t, n)$ 符号 $\Gamma(p_1, \dots, p_k'; n, t)$ は、その符号語 $w^{(1)}, \dots, w^{(n)}$ が次のように構成された符号であると定義する。

$w^{(u)}|_{Ci} = w^{(u \bmod pi)} \in \Gamma_0(p_i, t)$

ここで、 $C_i$ は構成要素の符号 $\Gamma_0(p_i, t)$ に対応するビット位置の集合である。この符号を $u$ 番目の利用者に割り当てるにすることにする。

## 【0146】

埋め込み符号生成のための符号化アルゴリズムは、次の通りである。

(符号化アルゴリズム)

- (1) 利用者識別番号  $u \in \{1, \dots, n\}$  を入力する。
- (2)  $i = 1$  から  $k'$  まで以下を実行する：
  - (2-1)  $u \bmod p_i$  を計算し、符号語  $w(u \bmod p_i) \in \Gamma_0(p_i, t)$  を生成する。

(3) 生成された符号語を連接して、一つの符号語  $W^{(u)}$  とする。

この符号化アルゴリズムにより生成された埋め込み符号の検出アルゴリズムとしては、先の検出アルゴリズム1を利用する。

## 【0147】

(定義3)  $\Gamma(p_1, \dots, p_{k'}; n, t)$  の構成要素に対して、検出アルゴリズム1を適用することで、高々2つの整数  $r_i^{(-)}, r_i^{(+)} \in Z_{p_i}$ を得る。ここで、 $0 \leq r_i^{(-)} \leq r_i^{(+)} \leq p_i$ である。

これらの整数  $r_i^{(-)}, r_i^{(+)} \in Z_{p_i}$  を  $\Gamma_0(p_i, t)$  の剩余(residues)と呼ぶことにする。また、集合  $\{r_i^{(-)}, r_i^{(+)}\}$  を  $\Gamma_0(p_i, t)$  の剩余対(residue pair)と呼ぶことにする。

## 【0148】

(定義4)  $r$  を  $\Gamma_0(p_i, t)$  の剩余とする。結託者の集合の中に  $r \equiv u \bmod p_i$  を満たす結託者が存在する場合、剩余  $r$  は  $u$  に起因する( $r$  arises from  $u$ )と呼ぶ。また、利用者が結託者であるか否かに関わらず、 $r$  が  $r \equiv u \bmod p_i$  を満足する場合、剩余  $r$  は  $u$  に起因する可能性がある(possibly arise from)と呼ぶ。

## 【0149】

(検出アルゴリズム2)

(1) 検出された符号  $x \in \{0, 1\}^L$  を入力する。ここで、 $L = (p_{ave} - 1)k't$  とする。

(2)  $x$  を  $k'$  個の制限  $x|_{C_i}, i = 1, \dots, k'$  個に分解する。

(3)  $i = 1$  から  $k'$  まで以下を実行する：

(3-1) 検出アルゴリズム1を  $x|_{C_i}$  に適用する。

(4) 全ての剩余の  $m$  組に対して以下を実行する：

(4-1) もし、剩余の  $m$  組が一貫しているならば、以下を実行する：

(4-2) その解を結託者として出力し中止する。

(5) 結託者が検出されなかつと出力する。

【0150】

(定理3)  $t \geq \log_2(4k' / \varepsilon)$  とする。以下の方程式が成立するとき、符号  $\Gamma(p_1, \dots, p_{k'}; t)$  は  $\varepsilon$  誤りを持った  $c$ -secure 符号である。

【0151】

【数13】

$$\left[1 - \left\{1 - \left(1 - \frac{1}{p}\right)^c\right\}^t\right]^{k' C_{k+1} \cdot 2^{k+1}} > 1 - \frac{\varepsilon}{2} \quad (6)$$

【0152】

このとき、符号サイズは、  $L = (p_{ave} - 1)k' \cdot t$  で与えられる。

【0153】

(補題4) 符号  $\Gamma(p_1, \dots, p_{k'}; n, t)$  の  $k'$  個の剩余対の中には、少なくとも  $2k' / c$  個の剩余を起因させている結託者が少なくとも 1 人存在する。

(補題4の証明) 符号  $\Gamma(p_1, \dots, p_{k'}; n, t)$  の  $k'$  個の剩余対に含まれる剩余は  $2k'$  個ある。平均すると、結託者 1 人あたり  $2k' / c$  個の剩余を起因させていることになる。従って、少なくとも 1 人の結託者は、  $2k' / c$  個以上の剩余を起因させている。

【0154】

(補題4の一般化)

補題4は、各部分符号から検出できる整数要素（剩余）の個数  $q$  を  $q = 2$  とした場合の例であるが、これを  $q$  を用いて一般化すると、次の通りとなる。

【0155】

(一般化した補題4の証明)

符号  $\Gamma(p_1, \dots, p_{k'}; n, t)$  の  $k'$  個の剩余  $q$  対（対ではないが、ここでは便宜上、そう呼ぶことにする）に含まれる剩余は、  $qk'$  個ある。平均すると結託者 1 人あたり、  $qk' / c$  個の剩余を起因させていることになる。従って、少なくとも 1 人の結託者は、  $qk' / c$  個以上の剩余を起因させている。

## 【0156】

ここで、結託者番号(結託者の利用者識別番号)の再構成と検定には、 $(k + 1)$  個の剩余が必要なので、一般化した補題4の結果より、 $q k' / c \geq k + 1$  が成立する必要がある。左辺の因子 $q / c$  を右辺に移すと、条件式 $k' \geq c(k + 1) / q$ を得る。

## 【0157】

(補題5)  $t \geq \log_2(2 k' / \varepsilon)$ とする。符号 $\Gamma(p_1, \dots, p_{k'}; n, t)$ に対して先の検出アルゴリズム1を適用するとき、 $k'$  個の剩余対の検出誤り率( $k'$  個の剩余対の中に、どの結託者にも起因しない剩余が含まれてしまう確率)は $\varepsilon$ 以下である。

## 【0158】

(補題5の証明) ある構成要素 $\Gamma_0(p_i, t)$ に対して検出アルゴリズム1を適用するときは、定理2より $t \geq \log_2(2 k' / \varepsilon)$ ならば、剩余対の検出誤り率は $\varepsilon / k'$  以下である。全部で $k'$  個の構成要素が存在するので、全ての剩余対に対する検出誤り率は $\varepsilon$ 以下である。

(補題6) ある一貫した剩余の $m$ 組が存在しており、これに別の因数 $q$ に対する剩余対からの剩余を加えて剩余の $(m + 1)$ 組を構成するとき、この $(m + 1)$ 組の剩余が偽に一貫している確率は、 $1 - (1 - 1/q)^c$ 以下である。

## 【0159】

(補題6の証明) 各剩余対は、全ての結託者の利用者識別番号に対する $q$ を法とする剩余のうちの最大値と最小値により構成されている。利用者は自分の利用者識別番号を知らないので、結託が行われたとき、ある利用者識別番号が結託者のものである確率は、利用者識別番号によらず一律であると考えられる。従って、ある結託者の剩余がある値をとる確率は、等しく $1 / q$ である。

## 【0160】

$c$ 人の結託者の剩余が全て一律に分布するとき、最大の剩余がある値 $c \in Z_q$ をとる確率 $Pr[x]$ は、以下のように与えられる。

## 【0161】

【数14】

$$\Pr[x] = \begin{cases} \left(1 - \frac{x}{q}\right)^c - \left(1 - \frac{x+1}{q}\right)^c & \text{for } x = q-1 \\ \left(\frac{1}{q}\right)^c & \text{for } x = q-1 \end{cases} \quad (7)$$

【0162】

(補題7) 以下の条件が成り立つとき、偽に一貫している剰余の( $k+1$ )組が存在する確率は次式に示すように  $\varepsilon$  以下である。

【0163】

【数15】

$$\left[1 - \left\{1 - (1 - 1/p)^c\right\}\right]^{c(k+l)/2 C_{k+l} \times 2^{k+l}} > 1 - \varepsilon \quad (8)$$

【0164】

(補題7の証明)  $k'$  個の剰余対から剰余の( $k+1$ )組を選択する組合せは  $\binom{k'}{k+1} C_{k+1} \times 2^{k+1}$  通りある。補題14から、剰余の( $k+1$ )組が偽に一貫している確率は、 $(1 - (1 - 1/q)^c)^{k'}$  である。従って、全ての組合せにおいて、少なくとも1個の偽に一貫している剰余の( $k+1$ )組が現れる確率は、次のような上限が与えられる。

【0165】

【数16】

$$P_F \leq 1 - \left[1 - \left\{1 - (1 - 1/p)^c\right\}\right]^{\binom{k'}{k+1} C_{k+1} \times 2^{k+1}} \quad (9)$$

【0166】

補題4の条件式が成立するとき、確率  $P_F$  は  $\varepsilon$  以下である。

## 【0167】

(定理3の証明) 潔白な利用者を誤って結託者であると検出する原因是、剩余対の検出誤りと偽に一貫している剩余の組の選択の二つがある。それぞれの確率を  $\varepsilon/2$  以下とするならば、検出誤り率は  $\varepsilon$  以下となる。補題5と補題7より、上の上限の式を得る。

偽に一貫している剩余の組を排除する確率を最小の因数で下限を抑える代わりに、小さい方から1個の因数を用いて下限を抑えることで、式(6)に代えて次式に示すような符号サイズのより小さな上限を得ることができる。

## 【0168】

## 【数17】

$$\left[ 1 - \prod_{i=1}^l \left\{ 1 - \left( 1 - \frac{1}{p_i} \right)^c \right\} \right]^{\frac{C_{k+l} \times 2^{k+l}}{2}} \geq 1 - \frac{\varepsilon}{2} \quad (10)$$

## 【0169】

ここで、  $p_1, \dots, p_{l'}$  は  $p_1, \dots, p_{k'}$  の中から選んだ1個(ただし、  $p_1 < p_2 < \dots < p_{l'}$  とする)であり、最も小さいものから順に選んだ1個であってもよいし、  $k+1$  番目から小さい順に最も大きい  $k+1$  番目まで選んだ1個であってもよいし、あるいは最も小さいものから  $k+1$  番目に小さいものまでの中から選んだ1個であってもよい。また、  $p_i$  ( $i = 1, 2, \dots, k'$ ) は  $c$  個の利用者識別番号に対して剩余計算部で計算される各剩余(整数要素)のとりうる値であり、本実施形態では前述の法記憶部  $21-1, 21-2, \dots, 21-k'$  で用意されている  $k'$  個の素数である。

## 【0170】

式(10)の意味について説明する。まず、式(10)の左辺は、検出が正しく結託者番号を特定する確率の下限を与えていた。つまり、左辺の大括弧の肩に乗っている「べき」は、  $k'$  個の剩余対から  $(k+1)$  個の剩余を選択してくる場合の例である。その個々の選択に対して、結託者番号が正しいか否かの判定を正しく

行う確率の加減が右辺全体の意味するところである。

#### 【0171】

ここで、式(10)左辺の大括弧の中身について詳しく説明する。上記の各選択では、結託者番号が正しいか否かを余分に1個の剩餘によって検定している。大括弧の中のΠによる積の部分は、1個の検定すべてが、誤った結託者番号を正しいとしてしまう確率の上限を与えている。なぜなら、各検定が誤った結託者番号を正しいと判定してしまう確率の下限は、(補題6)において、与えている確率 $1 - (1 - 1/q)^c$ において、各部分符号から検出できる整数要素(剩餘)の個数 $q$ (本実施形態では $q = 2$ )をその剩餘に対応する因数で置き換えたものによって与えられる。

#### 【0172】

検定に用いられる剩餘に対応する1個の因数は、最も小さな因数からなる組み合わせが $p_1, p_2, \dots, p_l$ の場合であって、この組み合わせが、誤った検定を行う確率の下限を最大にする組み合わせである。よって、Πによる積部分が1個の検定すべてが、誤った結託者番号を正しいとしてしまう確率の上限を与えていることになる。よって、式(10)は左辺であるところの正しい結託者番号を検出する確率の下限が右辺であるところの $1 - \varepsilon/2$ 以上であるための条件式を意味していることになる。

#### 【0173】

このように本実施形態によると、前述した一般化した補題4によって与えられる条件式 $k' \geq (k+1)/q$ を満たすように、より好ましくは式(10)を満足するように部分符号の数 $k'$ を規定することによって、結託攻撃への耐性を有し、かつ3人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成し、かつその埋め込み符号を正しく復号することができる。

#### 【0174】

##### (第3の実施形態)

次に、本発明の第3の実施形態として、ある条件の下で実現できる、第2の実施形態よりも短い符号サイズのc-secure符号による電子透かし埋め込み装置及び

検出装置について説明する。

【0175】

図11は、本実施形態に係る電子透かし埋め込み装置における埋め込み符号生成部の構成を示すブロック図である。この埋め込み符号生成部は、利用者識別番号を入力して同値類に基づく部分符号を生成する部分符号生成部61-1, 61-2, …, 61-k' と、これらの各部分符号を一つの符号に連接することによって、透かし情報である埋め込み符号を生成する符号連接部62からなる。

【0176】

図12に、図11の同値類に基づく部分符号生成部61-1, 61-2, …, 61-k' の一つ(61-i)の構成を示す。以下、 $Z_p = \{0, 1, 2, \dots, p-1\}$  とする。部分符号生成部61-iは、 $Z_p^k$ 内対応点計算部611と同値類要素番号計算部612及び部分符号生成部613によって構成される。

【0177】

$Z_p^k$ 内対応点計算部611は、利用者識別番号を入力して、対応する $Z_p^k$ 内の点を出力する。利用者識別番号ID(u)と $Z_p^k$ 内の点( $u_0, u_1, u_2, \dots, u_{p-1}$ )との対応付けは、例えば、 $u = u_0 + u_1 p + \dots + u_{k-1} p^{k-1}$ によって行う。ある集合Uの要素間に同値関係Rがあるとき、その同値関係Rによってある要素uと同値なものの全体の集合をその要素uの同値類と呼ぶ。Uの同値関係Rに関する同値類全体からなる集合をU/Rで表し、UのRに関する同値類という。 $Z_p^k$ の要素の間にある平行移動Tによって、同値関係 $R_T$ が定義できる。そして、この同値関係 $R_T$ に関する同値類が定義できる。

【0178】

一つの同値類に属する要素に対して、0から $p^{k-1}-1$ まで番号(これを同値類要素番号と呼ぶことにする)を割り振ることができる。同値類要素番号計算部612は、この同値類番号を計算して部分IDとして出力する。すなわち、本実施形態では入力された利用者識別番号に対する整数要素の組として、同値類要素番号計算部612により同値類要素番号が計算される。部分符号生成部613は、同値類要素番号計算部612で計算された部分IDから部分符号を生成する。

【0179】

図13は、平行移動による同値類の例を示す図である。これは  $p = 7$ ,  $k = 2$  の例である。平行移動(1, 6)と平行移動(3, 4)は、斜線部で示される格子によって構成されている同じ同値類を定義していることが分かる。

#### 【0180】

図14は、図13の  $p \times p$  の格子を周期的に繰り返したとき、同値類がどのように表されるかを示す図である。平行移動による同値関係によって定義される同値類であって、(0, 0)の格子を含む同値類は、ある傾きを持った直線上に乗っていることが分かる。図15は、図14を  $k = 3$  に拡張した場合の例を示す図である。同様にして、任意の正整数  $k$  に対して平行移動による同値関係によって同値類を定義することができる。

#### 【0181】

一つの同値類に含まれる元の個数は、 $p$  個である。順序番号(同値類内要素番号)は、この  $p$  個の元に対して与えられる。

一方、商集合の要素の個数(=同値類の個数)は  $p^k / p = p^{k-1}$  である。従つて、順序番号を指定すると、 $p^{k-1}$  個の元が指定されることになる。この順序番号が部分IDとして部分符号によって符号化されることになる。

#### 【0182】

ここで、同値類要素番号計算部612での同値類要素番号(部分ID)の割当て方法について述べる。この割当て方法として、次の2通りが考えられる。

#### 【0183】

(割当て方法1) 同値関係  $R_A$  に関する同値類に対して割り当てた番号である同値類番号を用いる方法であり、0から  $p^{k-1} - 1$  までの番号が割り当てられる。

#### 【0184】

(割当て方法2) 同値類の要素に対して割り当てた番号を用いる方法であり、0から  $p - 1$  までの番号が割り当てられる。

#### 【0185】

これらのうち割当て方法2がより好ましい。この割当て方法1を採用した場合には、第2の実施形態と同様の議論が展開できるため、先の式(6)が成立する。

つまり、式(6)と後述する式(27)の両者を満足するような符号を採用すれば良い。この割当て 方法2の例を挙げる。平行移動  $A_i = (a_{i,0}, a_{i,1}, \dots, a_{i,k-1})$  による同値類の場合、 $u = (u_0, \dots, u_{k-1})$  は、同値類要素番号(部分ID)として次式が割り当てられる。

【0186】

【数18】

$$\sum_{j=0}^{k-1} u_j a_{i,j} \bmod p \quad (11)$$

【0187】

図16に、本実施形態に係る電子透かし検出装置の構成を示す。この電子透かし検出装置は、透かし情報抽出部71、符号分割部72、同値類に基づく部分符号復号部73-1, 73-2, …, 73-k' 及び結託者番号計算部74から構成されている。

【0188】

透かし情報抽出部71では、入力された埋め込み済みコンテンツから透かし情報(埋め込み符号)が抽出され、この抽出された透かし情報である埋め込み符号が符号分割部72により各部分符号に分割された後、同値類に基づく部分符号復号部73-1, 73-2, …, 73-k' により復号されることにより、利用者識別番号に対応する同値類要素番号の対が生成される。こうして生成された各同値類要素番号の対から、結託者番号計算部74で結託者番号が計算され、結託者が特定される。

【0189】

なお、第1、第2の実施形態と同様に、同値類要素番号の対の一方から利用者識別番号計算部により利用者識別番号を計算で求め、また各同値類要素番号の対から結託判定部により結託の有無を判定し、その結託判定部判定結果について、結託判定OR部で論理和をとることにより、結託が存在したか否かを最終的に判定して、結託が存在すると判定されたときに結託者番号計算部74で結託者番号を計算する構成としてもよい。

## 【0190】

図17は、同値類に基づく部分符号復号部73-1, 73-2, …, 73-k'の一つ(73-i)の構成を示している。同値類に基づく部分復号部73-iは、後述するランダム誤りを許容する検出アルゴリズム3に基づくものであり、ブロック分割部730、“1”ビット計数部731、“ $>t_0$ ”判定部732、“ $< d - t_0$ ”判定部733、最小位置決定部734及び最大位置決定部735から構成される。

## 【0191】

ブロック分割部730は、入力された部分符号を各ブロックへ制限したものに分割して分割結果をそれぞれ“1”ビット計数部731へ出力する。“1”ビット計数部731は、“1”が立っているビットの数を計数して、その計数値を“ $>t_0$ ”判定部732及び“ $< d - t_0$ ”判定部733へそれぞれ出力する。

## 【0192】

“ $>t_0$ ”判定部732は、入力が第1の閾値 $t_0$ より大きいか否かを判定し、真ならば1、偽ならば0をそれぞれ出力する。“ $< d - t_0$ ”判定部733は、入力が第2の閾値 $d - t_0$ より小さいか否かを判定し、真ならば1、偽ならば0をそれぞれ出力する。

## 【0193】

最小位置決定部734は、“ $>t_0$ ”判定部732からの入力ビットの組のうち1が立っている最小のビット番号を出力する。最大位置決定部735は、“ $< d - t_0$ ”判定部733からの入力ビットの組のうち1が立っている最大のビット番号を出力する。

## 【0194】

ここで、図16の電子透かし検出装置において埋め込み符号である透かし情報の復号時に誤りが生ずる可能性がある場合について説明する。埋め込み符号の復号時に誤りがある場合には、誤った利用者を結託者と特定するおそれがある。この誤りを防ぐには2通りの方法がある。

## 【0195】

(方法1) 電子透かし埋め込み装置において、埋め込み符号に対して誤り訂正

符号化を行ってから埋め込みを行い、電子透かし検出装置において検出された符号に対して誤り訂正復号を行う。

(方法2) 図16の部分符号復号部 $73-1, 73-2, \dots, 73-k'$ に誤りを許容する性質を持たせる。

#### 【0196】

本実施形態では、(方法2)を採用する。抽出された埋め込み符号には誤り確率のランダムな誤りが加わっていると仮定する。第2の実施形態で述べた検出アルゴリズム1に改良を加えた以下のような検出アルゴリズム3を用いることで、誤りを許容する。

#### 【0197】

##### (検出アルゴリズム3)

(1) 検出された符号 $x \in \{0, 1\}^l$ を入力する。ここで、 $l = (n - 1)d$ とする。

(2)  $s = 0$ から $n - 2$ まで、以下を実行する：

(2-1)もし、 $\text{weight}(x | B_s) > 0$ ならば、中斷する。

(3)  $t = n - 1$ から $s$ まで、以下を実行する：

(3-1)もし、 $\text{weight}(x | B_{t-1}) < d - t_0$ ならば、中斷する。

(4)  $s$ と $t$ を出力する。

ここで $t_0$ は、この検出アルゴリズム3の誤りに対する許容性を表すパラメータである。

#### 【0198】

次に、結託による埋め込み符号の改竄があったことを判定する閾値として、新たなパラメータを加える意味について説明する。

埋め込み符号のうち、結託によっては改竄んが行われなかったブロックに対して、結託以外の原因でランダムな誤りが発生した場合、 $t_0 + 1$ ビット以上の反転が生ずる確率は、次式で与えられる。

#### 【0199】

## 【数19】

$$\varepsilon_1 = \sum_{i=t_0+1}^d d C_i (1-\varepsilon_0)^{d-i} \varepsilon_0^i < e^{-\frac{(t_0-d\varepsilon_0)^2}{d}} \quad (12)$$

## 【0200】

一方、結託によって改竄が行われたブロックに対して、結託以外の原因でランダムな誤りが加法的に加わった場合、 $t_0$ ビット以下の反転が生ずる確率は、次式より小さい。

## 【0201】

## 【数20】

$$\varepsilon_2 = \sum_{i=0}^{t_0} d C_i (1/2)^d < e^{-\frac{\left(\frac{d-t_0}{2}\right)^2}{d}} \quad (13)$$

## 【0202】

ランダム誤りのために埋め込み符号を誤って検出をしてしまう確率は、少なくとも一つのブロックにおいて誤った検出をする確率以下であり、この確率は、

$$\varepsilon_3 = 1 - (1 - \varepsilon_1)^{n-1} (1 - \varepsilon_2)^2 < (n-1) \varepsilon_1 + 2 \varepsilon_2$$

で表される。図18に示すように $t_0$ を適当に選択することで、加法的にランダムな誤りが加わった場合にも、検出誤りを小さく設定できる。

図17に示した部分符号復号部73-iは、上述したようなランダム誤りを許容する先の検出アルゴリズム3に基づく処理を行う。

## 【0203】

図19に、結託者番号計算部74の構成を示す。結託者番号計算部74は、同値類選択部81、一貫性検査部82及び候補ID計算部83から構成される。

## 【0204】

同値類要素選択部81は、 $k'$ 個の同値類要素番号の対の各々から一方の同値類番号を選択して一貫性検査部82へ出力し、一貫性検査部82から次候補の要

求を受けると、同値類要素番号の新たな組を選択する。

## 【0205】

一貫性検査部82は、 $k'$ 個の組から $(k+1)$ 個の組を選択し、その同値類要素番号の組が真に一貫しているか否かを検査する。この検査は、 $(k+1)$ 個のうち $k$ 個の同値類要素番号を候補ID計算部83に渡し、返された候補IDが残りの同値類要素番号の示す同値類番号と矛盾していないか否かを判定することにより行われる。残りの個のすべての同値類番号に対して、この判定が矛盾していないという結果ならば、この候補IDを結託者番号として出力し、そうでない場合には、次候補を一貫性検査部82に要求する。

## 【0206】

ここで、図19中の候補ID計算部83において $k$ 個の同値類要素番号から結託者番号を再構成する方法を示す。例えば、 $k$ 個の平行移動 $A_i(0), \dots, A_i(k-1)$ に対して、同値類要素番号が $r_0, \dots, r_{k-1}$ で与えられた場合、次式の連立合方程式が成り立つ。

## 【0207】

## 【数21】

$$\sum_{j=0}^{k-1} u_j a_{i(v),j} \equiv r_v \pmod{p} \quad (14)$$

## 【0208】

$k$ 次正方形行列( $a_{i(v),j}$ )が正則ならば、逆行列( $a^{-1}_{j,i(v)}$ )が存在する。この場合、次式によって利用者識別番号が得られる。

## 【0209】

## 【数22】

$$u_j = \sum_{v=0}^{k-1} a^{-1}_{j,i(v)} r_v \pmod{p} \quad (15)$$

## 【0210】

一般には、正則性が満たされるとは限らない。正則性が満足されない場合には

、利用者識別番号は一意に決まらず、結託者番号を含む利用者識別番号の集合が得られる。この集合は、 $p$  のべき乗の大きさを持つ。正則性を満たさない部分符号の組はあらかじめ分かっているので、結託者 ID の候補の計算には、選択しないような構成もできる。

## 【0211】

図19中の一貫性検査部82は、こうして得られた結託者番号の候補(を含む集合に対して)と、さらに1個の同値類要素番号 $r_k, \dots, r_{k+1-1}$ との間の一貫性を検証する。それは、 $v = 0, \dots, 1 - 1$ に対して、次式が成立することを確認することで行われる。

## 【0212】

## 【数23】

$$\sum_{j=0}^{k-1} u_j a_{i(k+v),j} \equiv r_{k+v} \pmod{p} \quad (16)$$

## 【0213】

本実施形態によると、第2の実施形態と同様に結託攻撃への耐性を有し、かつ3人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成し、かつその埋め込み符号を正しく復号することが可能となる。以下、詳細に説明する。

## 【0214】

まず、 $p$  を正整数とする。すなわち、本実施形態では第2の実施形態における $p_i$  ( $i = 1, 2, \dots, k'$ ) (所定個数 $n$ の利用者識別番号に対して計算される剰余の値の個数)に相当する個数 (所定個数 $n$ の利用者識別番号に対して計算される整数要素の値の個数) を同一の正整数 $p$  としている。そして、利用者識別番号 $u$ を $u = u_0 + u_1 p + \dots + u_{k-1} p^{k-1}$ に従って、 $(u_0, u_1, \dots, u_{k-1}) \in Z_p^k$ で表現する。また、 $k' = c(k+1)/2$ とし、 $p^k \geq n$ とする。

## 【0215】

空間 $Z_p^k$ の平行移動 $A \equiv (a_0, a_1, \dots, a_{k-1})$ に関する同値関係 $R_A$ を以下のように定義する。

## 【0216】

$$R_A((u_0, u_1, \dots, u_{k-1}), ((u'_0, u'_1, \dots, u'_{k-1}))$$

$$\longleftrightarrow u'_0 \equiv u_0 + a_0 \pmod{p},$$

$$u'_1 \equiv u_1 + a_1 \pmod{p} \dots,$$

$$u'_{k-1} \equiv u_{k-1} + a_{k-1} \pmod{p}$$

$jA - (j a_0 \pmod{p}, j a_1 \pmod{p}, \dots, j a_{k-1} \pmod{p})$  とすると、 $j$  が  $\gcd(j, p) = 1$  を満たすときには、 $R_A$  と  $R_{jA}$  とは同じ同値関係を与える。

## 【0217】

利用者全体の集合を  $U = Z_p^k$  の同値関係  $R_A$  に関する商集合  $U/R_A$  が定義できる。この商集合の個々の元は同値類と呼ばれ、同値関係  $R_A$  によって同一視された元の集合である。すべての同値類に対して、それに含まれる元に順序番号を与えることにより、ある番号を指定することで、各同値類から 1 個ずつ元を選択できる。

## 【0218】

$k'$  ( $k' \geq k$ ) 個の平行移動  $A_0, \dots, A_{k'-1}$  を用意すると、それぞれに対して商集合  $Q_i = U/R_{Ai}$  ( $i = 0, \dots, k'-1$ ) が定義される。各商集合に対して、上に述べた順序番号を定義する。

## 【0219】

次に、 $k'$  個の商集合中の任意の  $k$  個の商集合のそれぞれに対して、順序番号を指定することで、利用者を一意に特定できるような商集合の組を構成するために、以下のような条件を仮定する。

## 【0220】

(条件 1) 商集合の大きさを等しいとする。すべての  $A_i = (a_{i,0}, \dots, a_{i,k-1})$  ( $i = 0, \dots, k'-1$ )において、すべての  $a_{i,m}$  ( $m = 0, \dots, k-1$ ) に対して、 $\gcd(a_{i,m}, p) = 1$  または  $a_{i,m} = 0$  であるとする。これにより、 $jA_i = (0 \pmod{p}, \dots, 0 \pmod{p})$  を満たす最小の正整数  $j$  は  $p$  となる。

(条件 2) 2 つの平行移動  $A_i, A_i'$  に対して、 $jA_i = j'A_i'$  が成立する正整数  $j < p, j' < p$  が存在しない。

$p$  が素数の場合、このような条件を満たす平行移動の個数は、次のように数え

上げることができる。

まず、(条件1)より各平行移動の成分の値が  $p$  と互いに素である場合の数は、 $\phi(p) = p - 1$  で表される。ここで、 $\phi$  はオイラー関数である。これに 0 である場合を加えて、各成分がとりうる値の場合の数は、 $p$  である。従って、平行移動として許される場合の数は、 $(p^k - 1)$  個である。ここで、 $-1$  は、 $(0, 0, \dots, 0)$  を除外したことによる。ところが、これらの中には  $(p - 1)$  個ずつ互いに他の整数倍(1倍、2倍、…、 $(p - 1)$ 倍)となっているものがある。従って、実際に、相異なる商集合を定義する平行移動として独立なものは、 $(p^k - 1)/(p - 1)$  個となる。

### 【0221】

また、(条件2)に関しては、仮にある2つの平行移動  $A_i, A_{i'}$  が(条件2)の制約を満たさないとする。つまり、正整数  $j < p, j' < p$  に対して  $j A_i = j' A_{i'}$  とすると、 $p$  が素数の場合には、これは互いに他の整数倍で表現できることを意味する。よって、(条件1)に対して数え上げた独立な平行移動は、そのまま(条件2)を満足する。

平行移動の組は、次のように具体的に構成できる。

### 【0222】

#### 【数24】

$$\begin{aligned}
 A_1 &= (0, 0, \dots, 0, 1), \\
 A_2 &= (0, 0, \dots, 0, 1, 0), \\
 &\vdots \\
 A_{1+p} &= (0, 0, \dots, 0, 1, p-1), \\
 A_{1+p+1} &= (0, 0, \dots, 0, 1, 0, 0), \\
 &\vdots \\
 A_{1+p+p^2} &= (0, 0, \dots, 0, 1, p-1, p-1), \\
 &\vdots \\
 A_{1+p+p^2+\dots+p^{k-2}+1} &= (1, 0, \dots, 0), \\
 &\vdots \\
 A_{1+p+p^2+\dots+p^{k-1}} &= (1, p-1, \dots, p-1).
 \end{aligned} \tag{17}$$

### 【0223】

$p$  が素数でない場合についても、(条件1)(条件2)を満足するように平行移動

を選択すれば、同様の構成が可能である。

## 【0224】

上述したような平行移動の組によって商集合を構成し、各商集合の同値類の元に順序番号を定義することで、中国剰余定理に基づく符号の場合と同様の符号を構成できる。この符号が誤り  $\varepsilon$  を持つc-secure符号となるためには、定理3が成立することに加えて、以下の条件が満たされなければならない。

## 【0225】

## 【数25】

$$k' = \frac{c}{2}(k+l) \leq \frac{p^k - 1}{p-1} \quad (18)$$

## 【0226】

この場合、全ての因数は同じ大きさの  $p$  であるので、 $p_{ave} = p$  である。

## 【0227】

このように本実施形態によると、部分符号として式(17)で示されるような平行移動によって定義される同値類に基づく符号を生成して、この部分符号を連接することで、第1、第2の実施形態よりも短い符号サイズのc-secure符号による埋め込み符号を生成し、その埋め込み符号を検出する場合において、第2の実施形態で規定した条件式  $k' \geq c(k+1)/q$  や式(10)の条件に加え、さらに式(27)の条件を満足するようにすることによって、結託攻撃への耐性を有し、かつ3人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成し、かつその埋め込み符号を正しく復号することができる。

## 【0228】

## (第4の実施形態)

次に、本発明の第4の実施形態として、埋め込み済みコンテンツの品質への影響を小さく抑えるように、従来よりも最適な符号化が行われる電子透かし埋め込み装置及び検出装置について説明する。

## 【0229】

図22に、本実施形態に係る電子透かし埋め込み装置の構成を示す。この電子透かし埋め込み装置は、シンプレックス符号生成部91、符号語選択部92及び電子透かし埋め込み部93から構成されている。

#### 【0230】

シンプレックス符号とは、符号長 $n - 1$ 、符号語数nで、符号語間の相互相関が $-1/(n - 1)$ となる符号であり、n次のアダマール(Hadamard)行列を基に構成することができる。すなわち、符号語がn-1次元ユークリッド空間中のn-1次元単体の頂点に位置するような符号がシンプレックス符号である。例えば、3次元ユークリッド空間の場合は、図21に示すように(-1,-1,1), (1,-1,-1), (-1,1,-1)で示す3つの頂点に位置する符号がシンプレックス符号を構成する。

#### 【0231】

シンプレックス符号生成部91では、このようなシンプレックス符号の符号語を生成する。シンプレックス符号生成部91は、あらかじめ生成された符号語の表を記憶したものであってもよい。符号語選択部92は、生成されたシンプレックス符号に順番を割り振っておき、与えられた利用者識別番号に対応する符号語を選択して出力する。なお、シンプレックス符号生成部91及び符号語選択部92の部分は、利用者識別番号が入力されてから、利用者識別番号に対応するシンプレックス符号の符号語を生成して出力するように構成されていてもよい。

#### 【0232】

電子透かし埋め込み部93は、符号語選択部92より受け取った符号語を透かし情報として埋め込み対象コンテンツに埋め込む。埋め込みは、スペクトラム拡散によって行う。

#### 【0233】

図23に、図22に示した電子透かし埋め込み装置に対応する本実施形態に係る電子透かし検出装置の構成を示す。この電子透かし検出装置は、シンプレックス符号生成部101、符号語選択部102、相関値計算部103及び相関値判定部104から構成されている。シンプレックス符号生成部101と符号語選択部102については、図22で説明した電子透かし埋め込み装置の中のそれと同一であるため、説明を省略する。

## 【0234】

相関値計算部103では、入力された埋め込み済みコンテンツと入力された利用者識別番号に基づいて符号選択部102で選択された符号語との間の相関値を計算する。相関値判定部104では、相関値計算部103により計算された相関値がある閾値を超えているか否かによって、符号選択部102からの符号語が埋め込み済みコンテンツに埋め込まれているか否かを判定し、検出／非検出信号を出力する。

## 【0235】

このように本実施形態に係る電子透かし埋め込み／検出装置によれば、任意の対の間での相互相関値が小さくなるようなシンプレックス符号の符号語を擬似乱数系列として用い、これを透かし情報として埋め込んでいる。従って、透かし情報として別の利用者識別番号に対応する符号語が埋め込まれていると誤判定を行う確率は非常に小さくなる。

## 【0236】

## (第5の実施形態)

次に、本発明の第5の実施形態として、第4の実施形態の電子透かし検出装置を応用して結託攻撃に対する結託者特定機能を持たせた電子透かし検出装置について説明する。図24は、本実施形態に係る結託者特定機能に係る部分の構成を示している。

## 【0237】

この電子透かし検出装置は、結託者特定機能を持たせるために、シンプレックス符号生成部111、符号語選択部112、相関値計算部113、利用者識別番号生成部114、相関値ベクトルノルム計算部115、電子透かし判定部116及び結託者判定部117を有する。シンプレックス符号生成部111、符号語選択部112及び相関値計算部113は、図23に示した電子透かし検出装置の中のそれと基本的に同じである。

## 【0238】

利用者識別番号生成部114では、予め登録されたすべての利用者識別番号を生成する。符号語選択部112では、これらすべての利用者識別番号に対応する

シンプレックス符号の符号語が選択され、これらの各符号語と図示しない埋め込み済みコンテンツとの相関値が相関値計算部113で計算される。

#### 【0239】

相関値ベクトルノルム計算部115では、すべての利用者識別番号に対して計算された相関値をベクトルとみなして、そのノルムを計算する。この相関値ベクトルノルムは、例えばすべての相関値の和とする。

#### 【0240】

電子透かし判定部116では、計算されたベクトルノルムに基づいて、例えば、このノルムがある閾値を超えるか否かにより、透かし情報が埋め込まれていたか否かを判定する。この判定の結果、透かし情報が埋め込まれていたと判断した場合には、結託者判定部117において相関値ベクトルの中で最も大きな値を示した利用者識別番号を保有する利用者を結託者として特定する。

#### 【0241】

また、結託者特定部117においては、このような方法の他、例えば相関値ベクトルが $n - 1$ 次元単体の部分単体のうち、どの部分単体の重心を通るかを求め、その部分単体の頂点に対応する利用者識別番号を保有する利用者を結託者とすることで、複数の結託者を特定することもできる。

#### 【0242】

なお、第4乃至第5の実施形態において、透かし情報として用いる擬似乱数系列として、 $N(0, 1)$ のガウシアンノイズを採用する場合には、図25に示すようにシンプレックス符号生成部121で生成されたシンプレックス符号をランダム座標回転部122によりランダムに回転させて符号語とすればよい。

#### 【0243】

さらに、本発明に係る埋め込み符号生成装置は、電子透かし埋め込み装置のようにデジタルデータである埋め込み対象コンテンツの透かし情報として埋め込むための埋め込み符号のみでなく、例えば化学物質からなる合成物などに化学的に埋め込むための埋め込み符号を生成するような用途にも適用できる。

#### 【0244】

#### 【発明の効果】

以上説明したように、本発明によればフィンガープリンティングシステムを構成する電子透かし埋め込み／検出装置において、利用者総数や結託者数が大きくなっても、小さな符号サイズの透かし情報を埋め込ことによってコンテンツの品質劣化を伴うことなく、結託攻撃に対するロバスト性を持つことができ、非可逆圧縮等の他の攻撃に対してもロバスト性を得ることができる。

#### 【0245】

また、本発明の電子透かし埋め込み／検出装置により、コピー制御情報や利用制御情報といった透かし情報を埋め込み、コンテンツを利用する機器を制御する場合に、同一コンテンツに対して異なる機器制御情報が埋め込まれている場合にその比較によって制御情報の改竄を行う攻撃に対してもロバスト性を有するコンテンツ利用システムを構築することも可能である。

#### 【0246】

さらに、本発明によると結託攻撃への耐性を有し、かつ3人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成する埋め込み符号生成装置及びその埋め込み符号を正しく復号する埋め込み符号検出装置を提供することができる。

#### 【図面の簡単な説明】

【図1】 本発明に係る電子透かし埋め込み装置及び電子透かし検出装置が適用されるフィンガープリンティングシステムの概略構成を示す図

【図2】 本発明の第1の実施形態に係る電子透かし埋め込み装置の構成を示すブロック図

【図3】 図2における埋め込み符号生成部の構成を示すブロック図

【図4】 図3における部分符号生成部の構成を示すブロック図

【図5】 本発明の第1の実施形態に係る電子透かし検出装置の構成を示すブロック図

【図6】 図5における結託者番号計算部の構成を示すブロック図

【図7】 図6における一貫性検査部の構成を示すブロック図

【図8】 同実施形態における結託者特定アルゴリズムを示すフローチャート

ト

【図9】 図5における中国剰余定理部の処理の流れを示すフローチャート

【図10】 同実施形態に係る電子透かし検出装置の処理の流れを示すフローチャート

【図11】 本発明の第3の実施形態に係る埋め込み符号生成部の構成を示すブロック図

【図12】 図11における同値類に基づく部分符号生成部の構成を示すブロック図

【図13】 同実施形態における平行移動による同値類によって商集合が定義できることを示す図

【図14】 同実施形態における平行移動による同値類の例を示す図

【図15】 同実施形態における  $k = 3$  の場合の同値類の例を示す図

【図16】 同実施形態に係る電子透かし検出装置の構成を示すブロック図

【図17】 図16における同値類に基づく部分符号復号部の構成を示すブロック図

【図18】 図17に示した同値類に基づく部分符号復号部について説明する図

【図19】 図16における結託者番号計算部の構成を示すブロック図

【図20】 本発明で生成される部分符号(結託前の部分符号)の値を示す図

【図21】 本発明の第4乃至第5の実施形態で使用するシンプレックス符号について説明する図

【図22】 本発明の第4の実施形態に係る電子透かし埋め込み装置の構成を示すブロック図

【図23】 本発明の第4の実施形態に係る電子透かし検出装置の構成を示すブロック図

【図24】 本発明の第5の実施形態に係る結託者特定機能を有する電子透かし検出装置の構成を示すブロック図

【図25】 本発明の第4乃至第5の実施形態におけるシンプレックス符号生成部の他の例を示すブロック図

【図26】 電子透かしに対する結託攻撃について説明する図

【図27】  $\Gamma_0(n, d)$  符号及びそれに対する結託攻撃を説明する図

【図28】  $\Gamma_0(n, d)$  符号における二つの符号間の最大距離と最小距離について説明する図

【図29】  $\Gamma_0(n, d)$  符号を用いた従来の電子透かしアルゴリズムにおける問題点を説明する図

【符号の説明】

1 1 …埋め込み符号生成部

1 2 …符号埋め込み部

2 1 - 1, 2 1 - 2, …, 2 1 - k' …法記憶部

2 2 - 1, 2 2 - 2, …, 2 2 - k' …剩余計算部

2 3 …符号パラメータ記憶部

2 4 - 1, 2 4 - 1, …, 2 4 - k' …部分符号生成部

2 5 …符号連接部

4 1 …透かし情報抽出部

4 2 …符号分割部

4 3 - 1, 4 3 - 2, …, 4 3 - k' …部分符号復号部

4 4 …利用者識別番号計算部

4 5 - 1, 4 5 - 2, …, 4 5 - k' …結託判定部

4 6 …結託判定OR部

4 7 …結託者番号計算部

5 1 …剩余選択部

5 2 …一貫性検査部

5 3 …中国剩余定理部

6 1 - 1, 6 1 - 2, …, 6 1 - k' …同値類に基づく部分符号生成部

6 2 …符号連接部

7 1 …透かし情報抽出部

7 2 …符号分割部

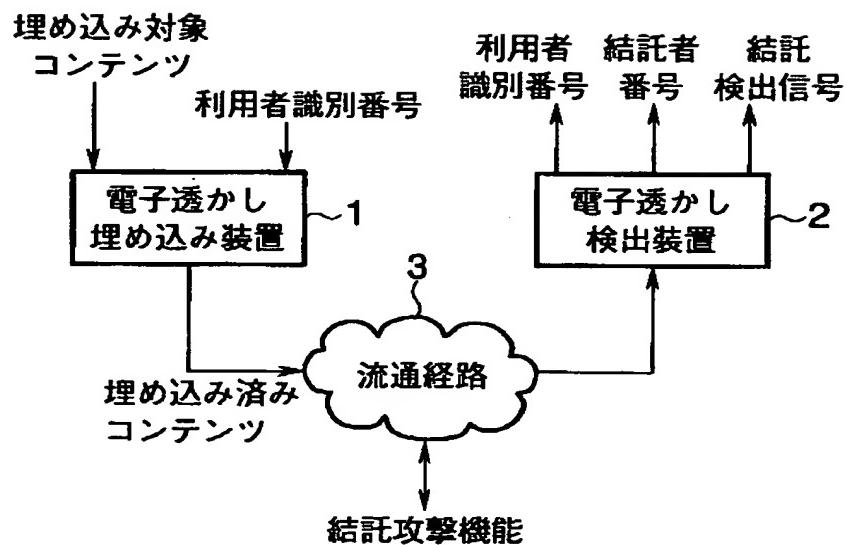
7 3 - 1, 7 3 - 2, …, 7 3 - k' …同値類に基づく部分符号復号部

7 4 …結託者番号計算部

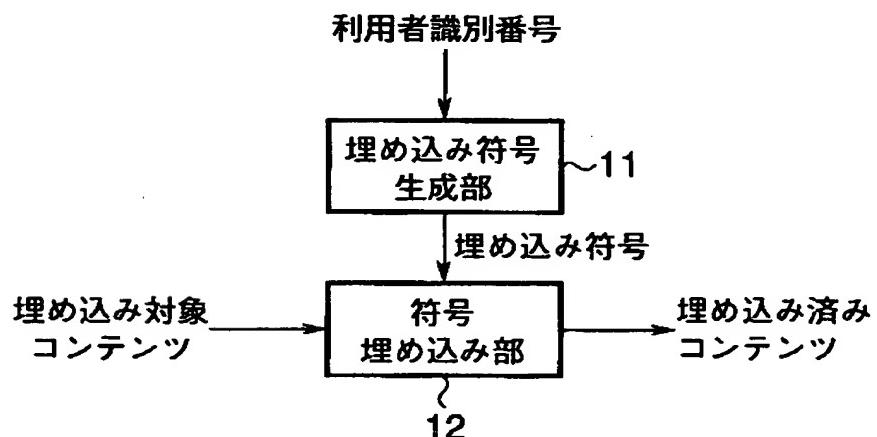
8 1 …同値類選択部  
8 2 …一貫性検査部  
8 3 …候補 I D 計算部  
9 1 …シングレックス符号生成部  
9 2 …符号語選択部  
9 3 …電子透かし埋め込み部  
1 0 1 …シングレックス符号生成部  
1 0 2 …符号語選択部  
1 0 3 …相関値計算部  
1 0 4 …相関値判定部  
1 1 1 …シングレックス符号生成部  
1 1 2 …符号語選択部  
1 1 3 …相関値計算部  
1 1 4 …利用者識別番号生成部  
1 1 5 …相関値ベクトルノルム計算部  
1 1 6 …電子透かし判定部  
1 1 7 …結託者特定部

【書類名】 図面

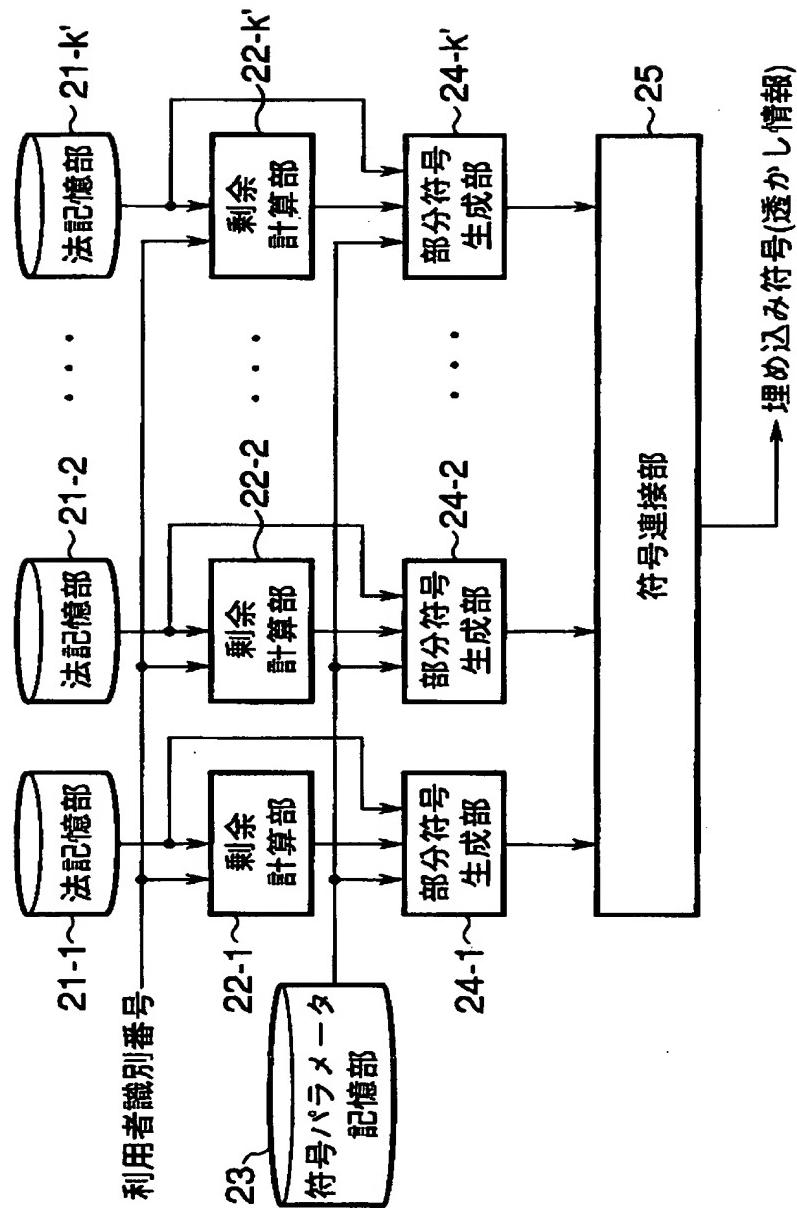
【図1】



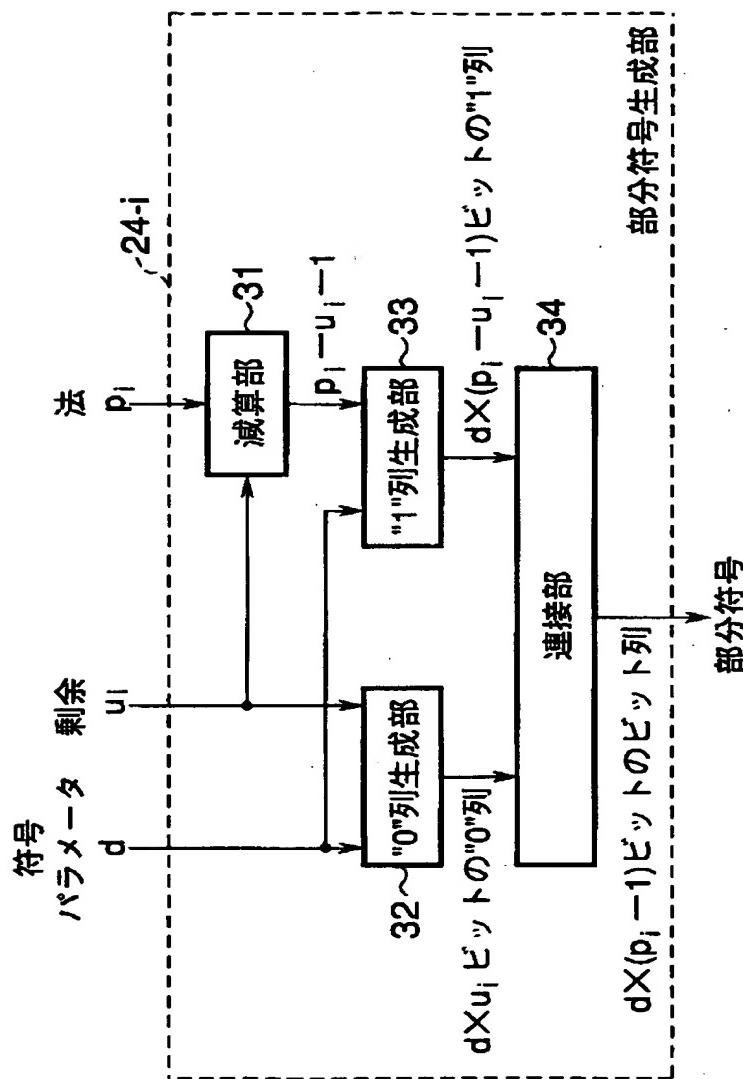
【図2】



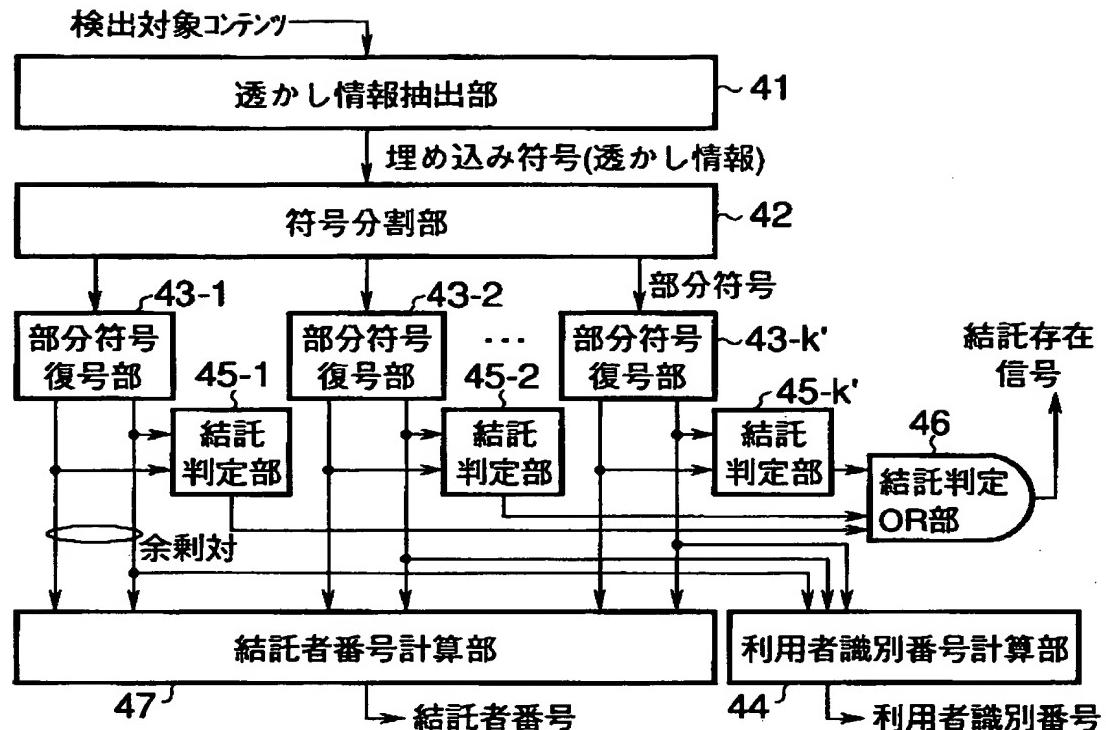
【図3】



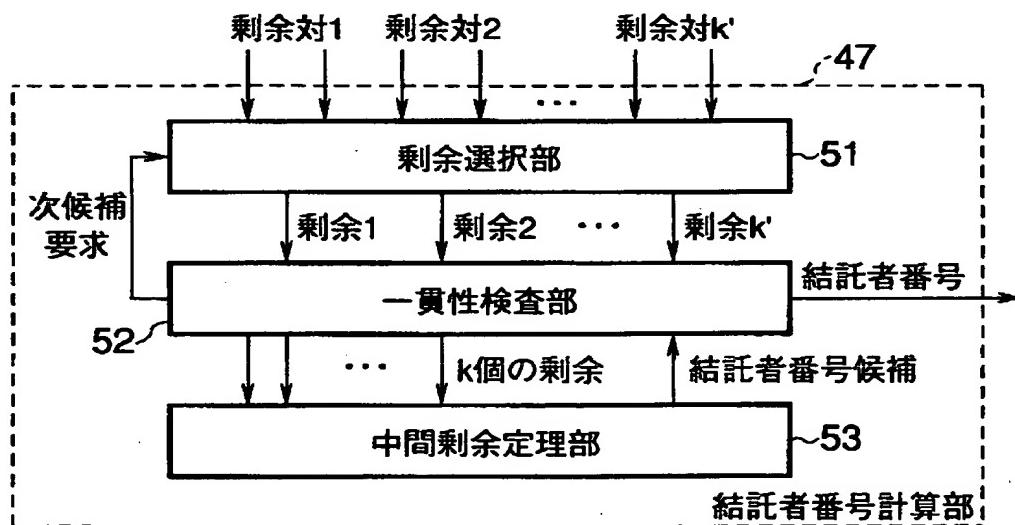
【図4】



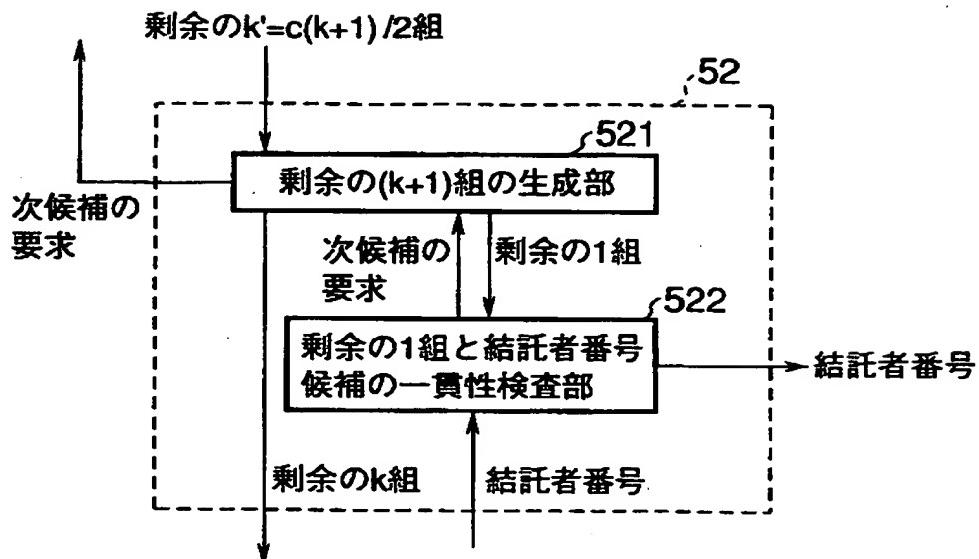
【図5】



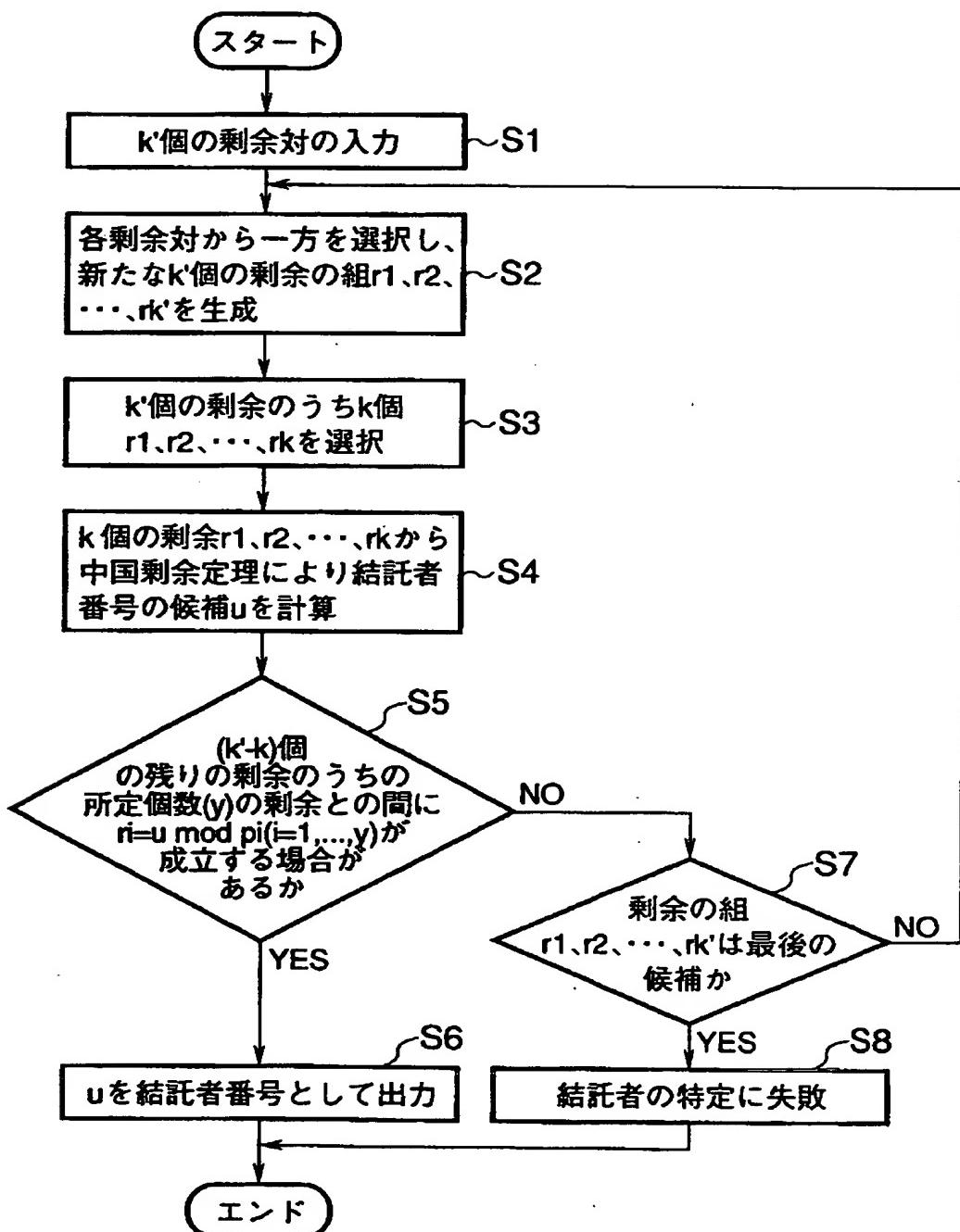
【図6】



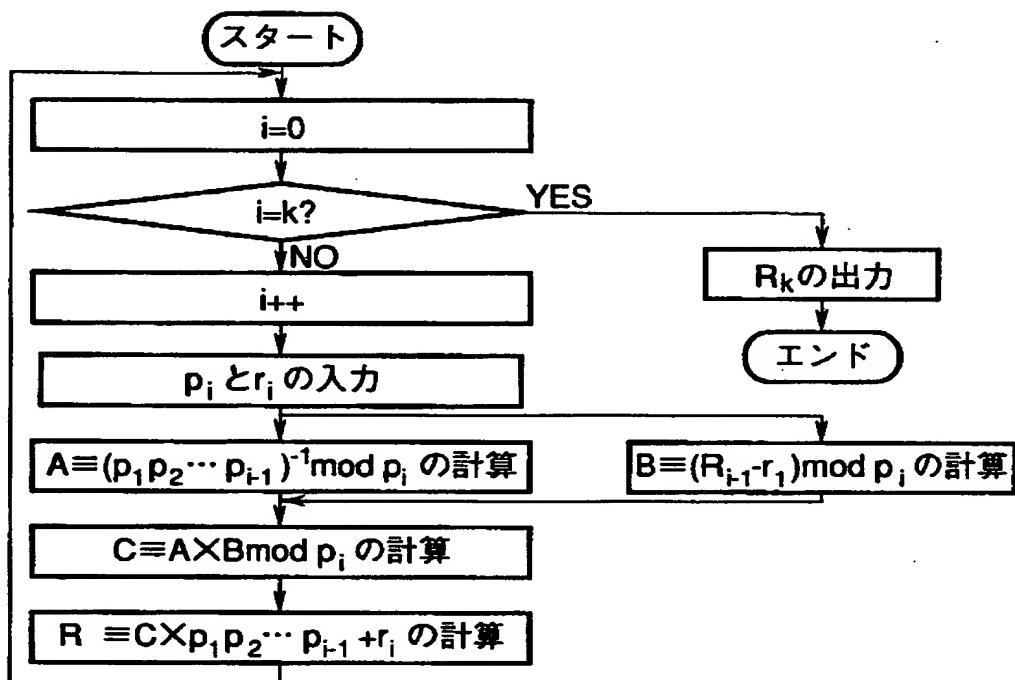
【図7】



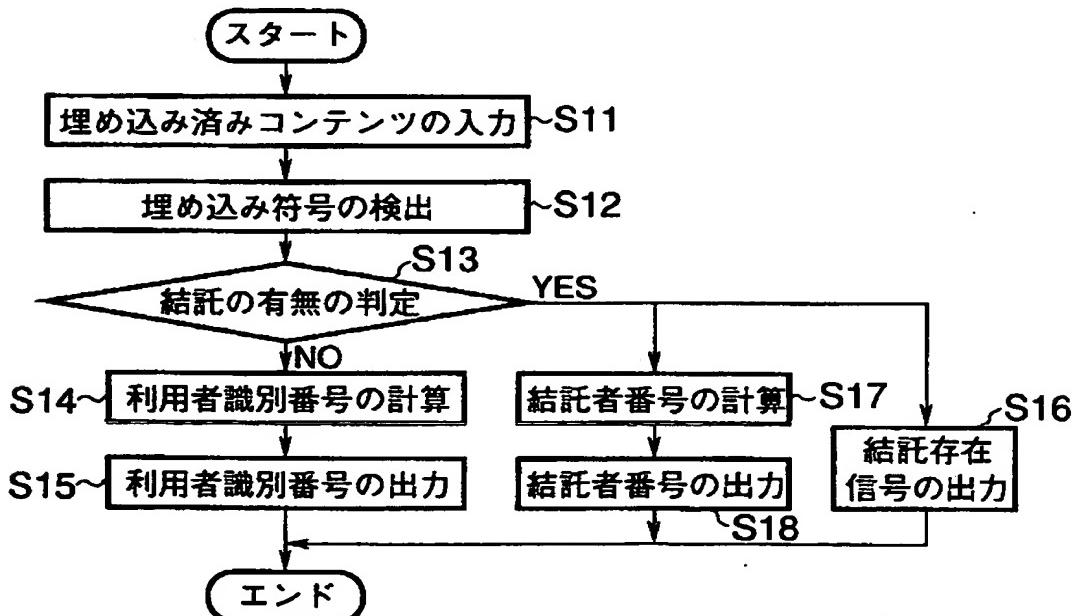
【図8】



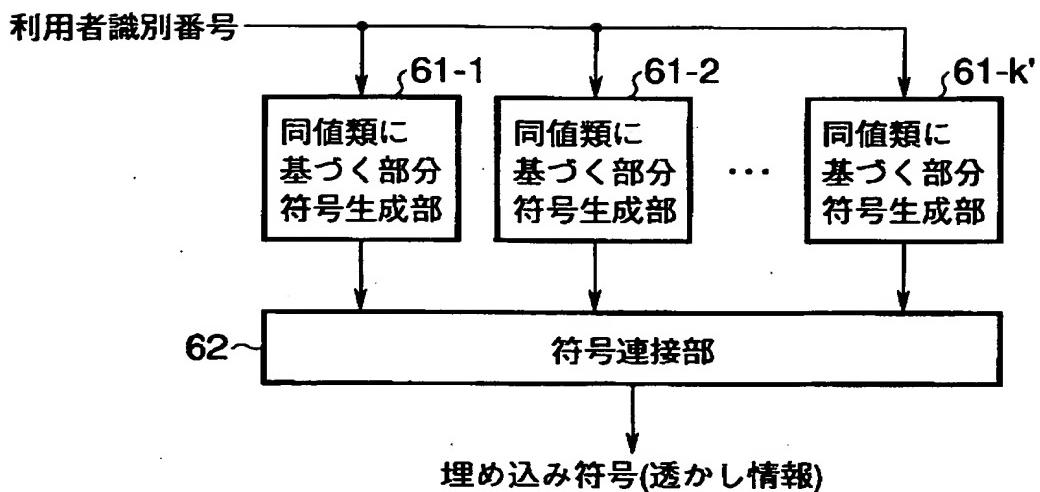
【図9】



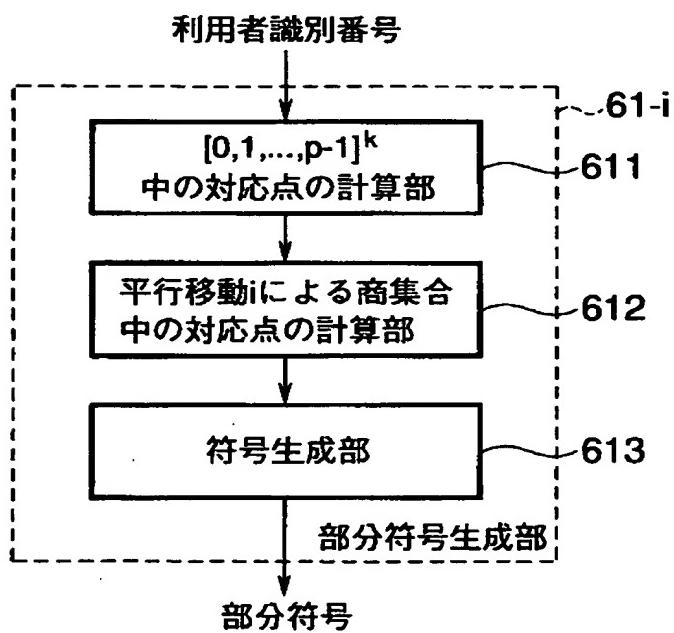
【図10】



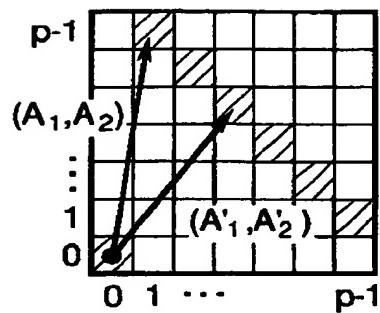
【図11】



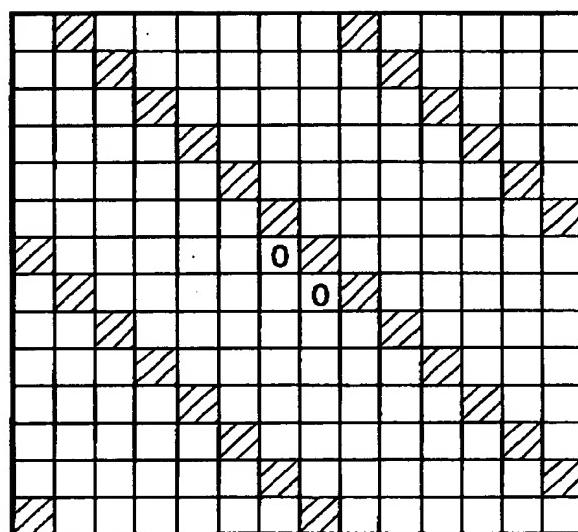
【図12】



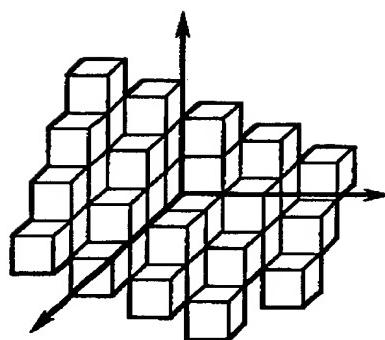
【図13】



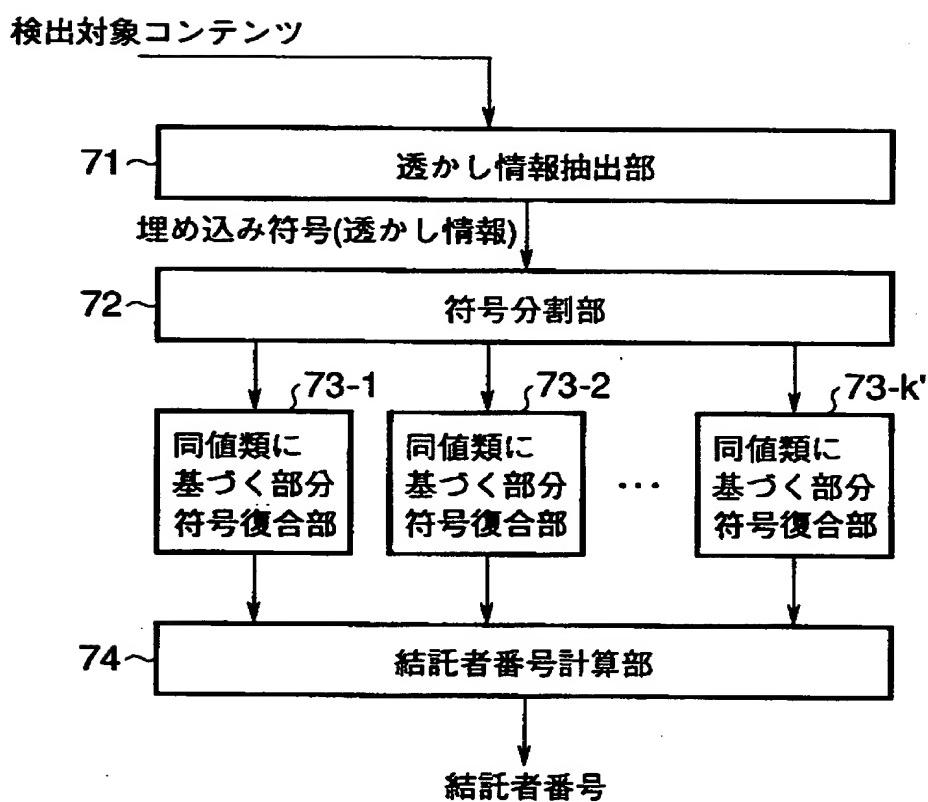
【図14】



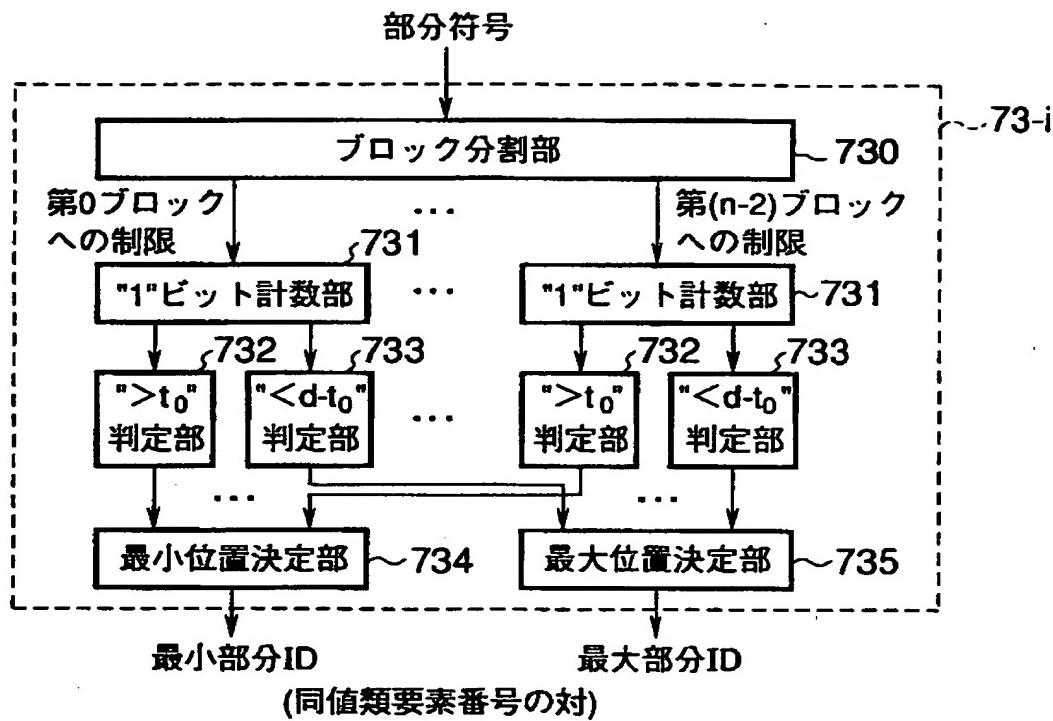
【図15】



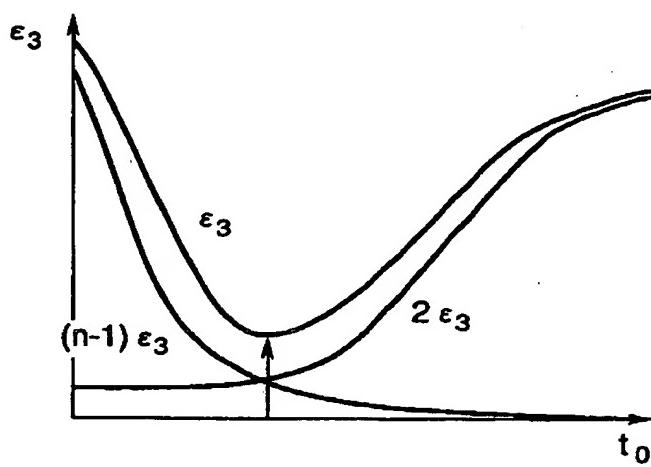
【図16】



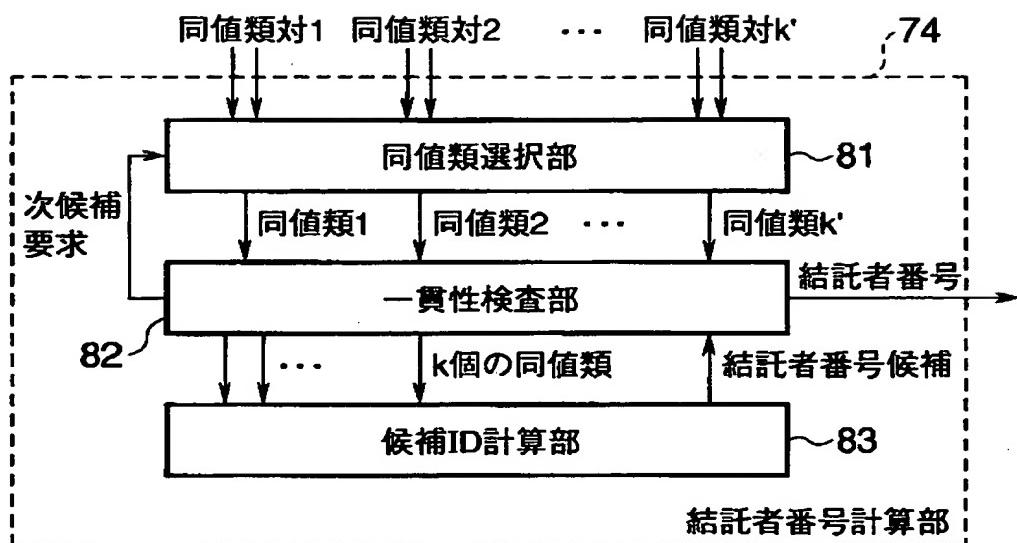
【図17】



【図18】

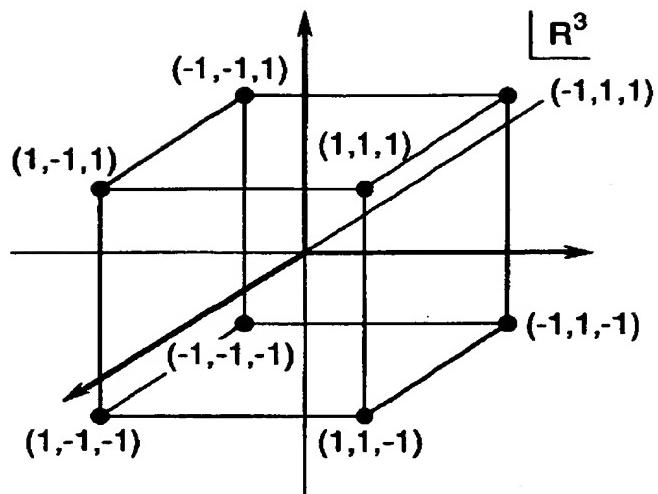


【図 19】

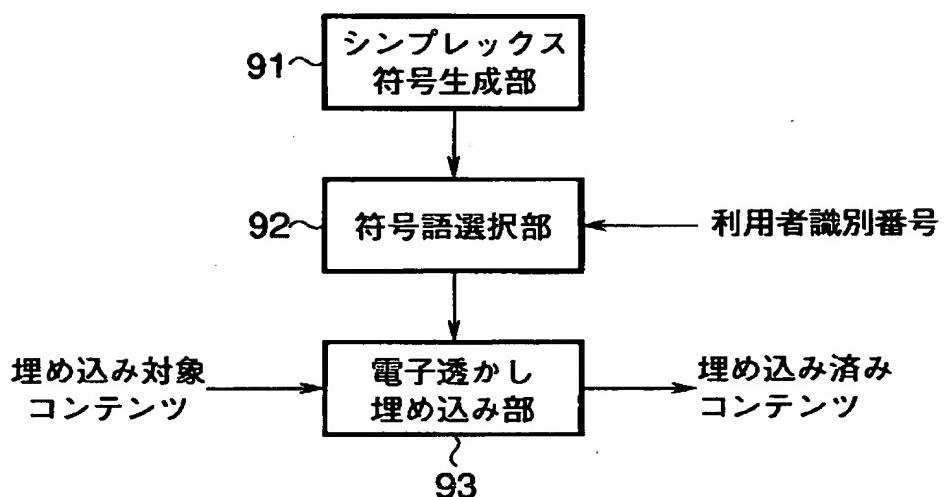


【図20】

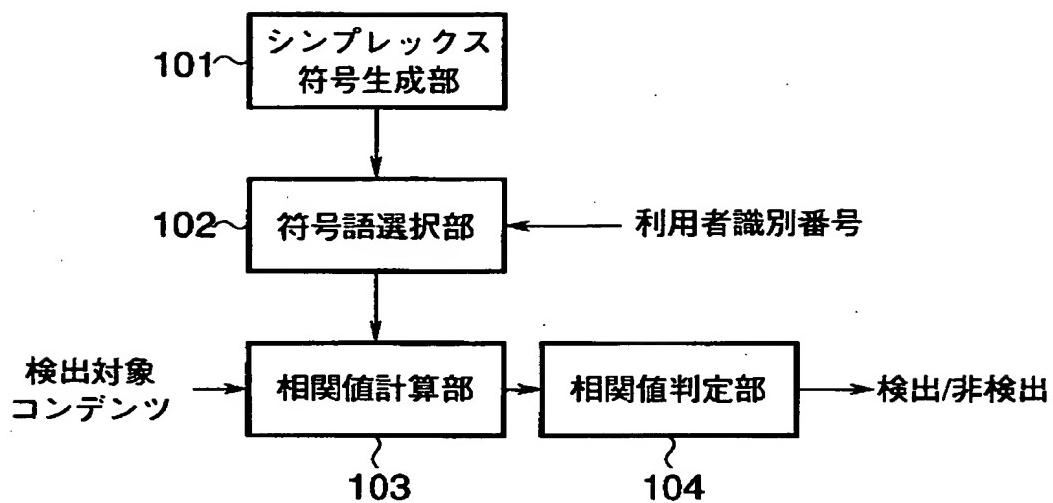
【図21】



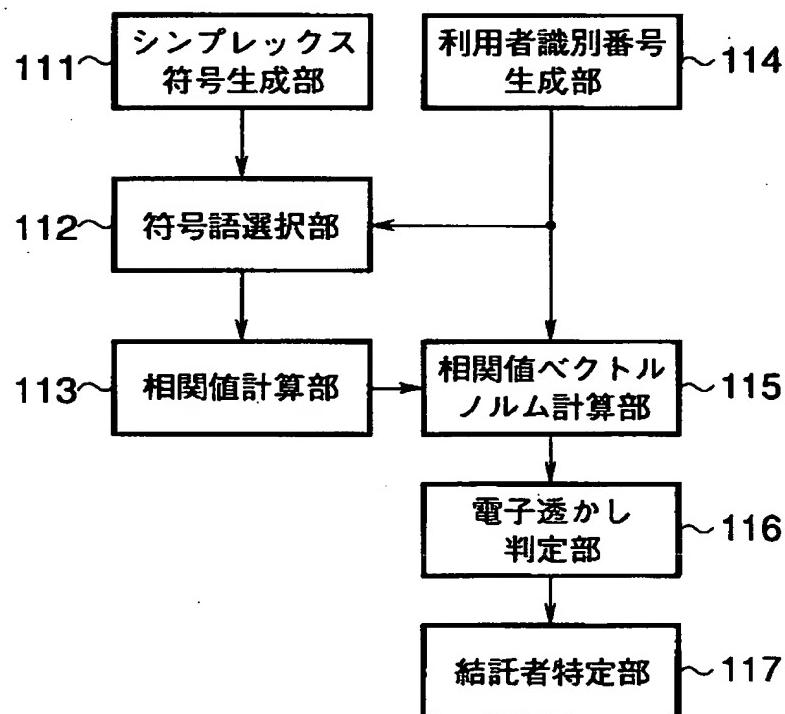
【図22】



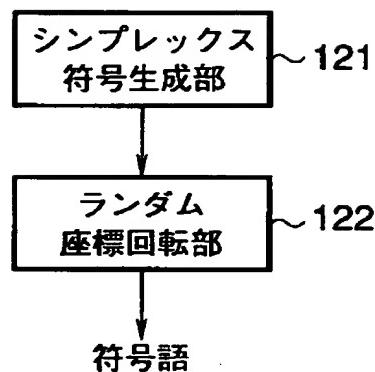
【図23】



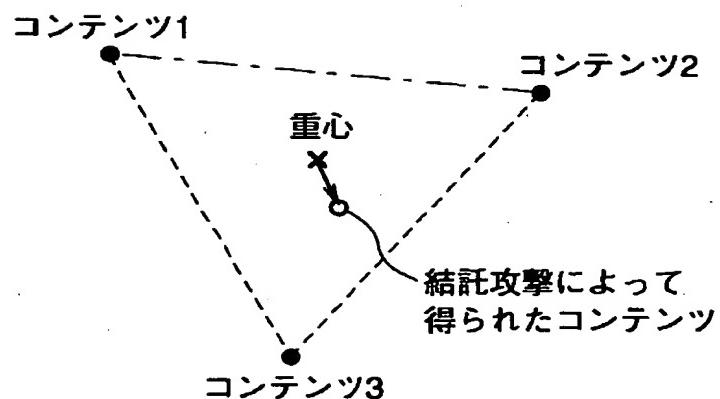
【図24】



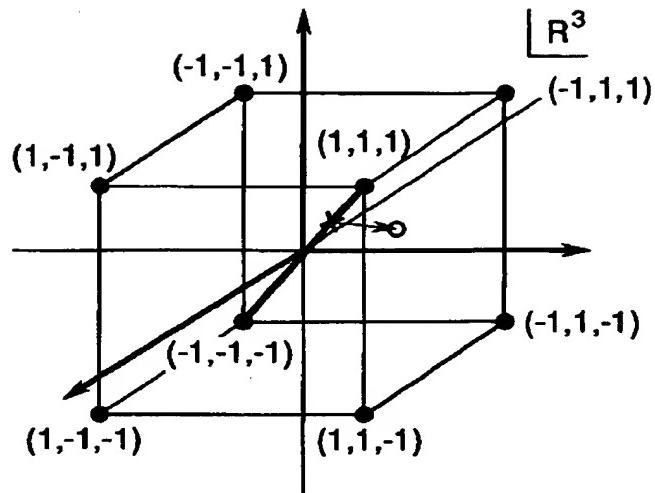
【図25】



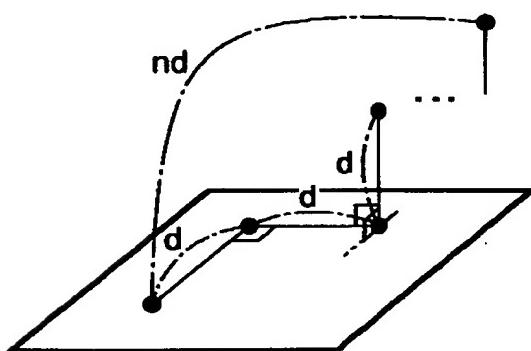
【図26】



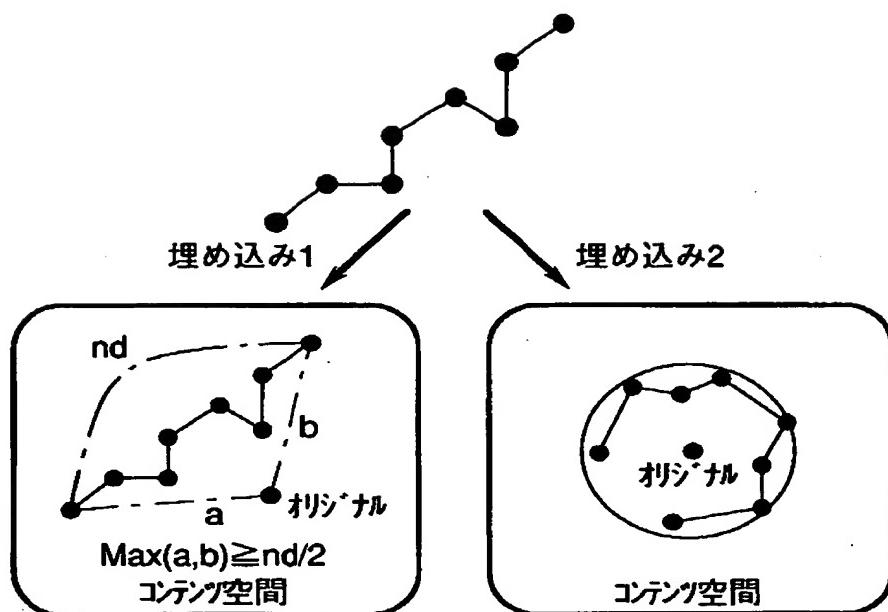
【図27】



【図28】



【図29】



【書類名】 要約書

【要約】

【課題】 結託攻撃への耐性を持ち、利用者総数や結託者総数が大きな場合においても、コンテンツの品質劣化を極力抑えて透かし情報を埋め込む電子透かし埋め込み装置を提供する。

【解決手段】 剰余計算部 22-1, 22-2, …, 22-k' により利用者識別番号に対して法記憶部 21-1, 21-2, …, 21-k' に記憶された複数の素数を法とする剰余をそれぞれ求め、これらの剰余及び符号化パラメータ記憶部 23 に記憶されたパラメータに基づいて、部分符号生成部 24-1, 24-2, …, 24-k' により所定のビット数を一単位とする連続した 1 の列及び 0 の列で構成される部分符号をそれぞれ生成し、これらの各部分符号を接続部 25 で接続して、透かし情報を構成する埋め込み符号を生成する。

【選択図】 図 3

出願人履歴情報

識別番号 [000003078]

1. 変更年月日 1990年 8月22日

[変更理由] 新規登録

住 所 神奈川県川崎市幸区堀川町72番地

氏 名 株式会社東芝